COMMITTEE OF EXPERTS ON THE EVALUATION
OF ANTI-MONEY LAUNDERING MEASURES AND
THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2018)17

Anti-money laundering and counter-terrorist financing measures

Czech Republic

Fifth Round Mutual Evaluation Report

December 2018

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The fifth round mutual evaluation report on Czech Republic was adopted by the MONEYVAL Committee at its 57th Plenary Session (Strasbourg, 3 – 7 December 2018).

Table of Contents

Key Findings 5
Risks and General Situation 7
Overall Level of Effectiveness and Technical Compliance 8
Priority Actions 15
Effectiveness & Technical Compliance Ratings 17

MUTUAL EVALUATION REPORT 18

Preface 18

CHAPTER 1. ML/TF RISKS AND CONTEXT 19

ML/TF Risks and Scoping of Higher-Risk Issues 19
Materiality 25
Structural elements 25
Background and other contextual factors 26

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION 35

Key Findings and Recommended Actions 35
Immediate Outcome 1 (Risk, Policy and Coordination) 36

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES 46

Key Findings and Recommended Actions 46
Immediate Outcome 6 (Financial intelligence ML/TF) 49
Immediate Outcome 7 (ML investigation and prosecution) 60
Immediate Outcome 8 (Confiscation) 71

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION 83

Key Findings and Recommended Actions 83
Immediate Outcome 9 (TF investigation and prosecution) 85
Immediate Outcome 10 (TF preventive measures and financial sanctions) 92
Immediate Outcome 11 98

CHAPTER 5. PREVENTIVE MEASURES 104

Key Findings and Recommended Actions 104
Immediate Outcome 4 (Preventive Measures) 105

CHAPTER 6. SUPERVISION 115

Key Findings and Recommended Actions 115
Immediate Outcome 3 (Supervision) 117

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS 138

Key Findings and Recommended Actions 138
Immediate Outcome 5 (Legal Persons and Arrangements) 139

CHAPTER 8. INTERNATIONAL COOPERATION 145

Key Findings and Recommended Actions 145
Immediate Outcome 2 (International Cooperation) 145

TECHNICAL COMPLIANCE ANNEX 155

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach 155
Recommendation 2 - National Cooperation and Coordination 158
Recommendation 3 - Money laundering offence 159
Recommendation 4 - Confiscation and provisional measures 162
Recommendation 5 – Terrorist Financing Offence 164
Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing 166
Recommendation 7 – Targeted financial sanctions related to proliferation 171
Recommendation 8 – Non-profit organisations 174
Recommendation 9 – Financial institution secrecy laws 179
Recommendation 10 – Customer due diligence 179
Recommendation 11 – Record-keeping 184
Recommendation 12 – Politically exposed persons 184
Recommendation 13 – Correspondent banking 186
Recommendation 14 – Money or value transfer services 186
Recommendation 15 – New technologies 187
Recommendation 16 – Wire transfers 188
Recommendation 17 – Reliance on third parties 191
Recommendation 18 – Internal controls and foreign branches and subsidiaries 192
Recommendation 19 – Higher-risk countries 193
Recommendation 20 – Reporting of suspicious transaction 193
Recommendation 21 – Tipping-off and confidentiality 195
Recommendation 22 – DNFBPs: Customer due diligence 195
Recommendation 23 – DNFBPs: Other measures 196
Recommendation 24 – Transparency and beneficial ownership of legal persons 197
Recommendation 25 – Transparency and beneficial ownership of legal arrangements 200
Recommendation 26 – Regulation and supervision of financial institutions 202
Recommendation 27 – Powers of supervisors 206
Recommendation 28 – Regulation and supervision of DNFBPs 207
Recommendation 29 - Financial intelligence units 209
Recommendation 30 – Responsibilities of law enforcement and investigative authorities 211
Recommendation 31 - Powers of law enforcement and investigative authorities 212
Recommendation 32 – Cash Couriers 214
Recommendation 33 – Statistics 216
Recommendation 34 – Guidance and feedback 217
Recommendation 35 – Sanctions 218
Recommendation 36 – International instruments 222
Recommendation 37 - Mutual legal assistance 223
Recommendation 38 – Mutual legal assistance: freezing and confiscation 227
Recommendation 39 – Extradition 229
Recommendation 40 – Other forms of international cooperation 230

SUMMARY OF TECHNICAL COMPLIANCE – KEY DEFICIENCIES 238

EXECUTIVE SUMMARY

1. This report provides a summary of the anti-money laundering (AML) and countering the financing of terrorism (CFT) measures in place in the Czech Republic as at the date of the on-site visit (5 to 16 March 2018). It analyses the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations and the level of effectiveness of the Czech Republic AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

The National Risk Assessment (NRA) appears to be the result of a transparent and realistic analysis of the money laundering (ML) and financing of terrorism (FT) risks faced by the country. However, certain aspects of risks identified in the NRA, such as laundering of foreign proceeds, the use of instruments of fictitious entrepreneurships, real estate business or risk posed by organised crime require further analysis. The private sector contributed, to a certain extent, in identifying key ML/FT risk and the Financial Analytical Unit (FAU) provided sector-specific versions of the NRA to the reporting entities, and prepared the general structure of the risk assessment which should be used by the private sector when performing their own evaluation of risks.

The Ministry of Interior developed the National Security Audit (NSA), which examines, inter alia, the risk related to terrorism, terrorism financing and organised crime. Since the NSA looks at several relevant areas, it remains unclear why the analysis therein was not fully integrated with the NRA. The specific levels and prioritisation of different categories of risks could have been expressed in a clearer manner such that the conclusions should have led the reader to easily establish the priorities as between different risk areas.

Competent authorities use financial intelligence produced by the FAU to a certain extent. Law enforcement agencies (LEAs) use other information (e.g. their own intelligence, complaints from the public and information gained in the course of investigating predicate offences) to initiate ML and FT investigations regularly. Whilst the statistics do not provide a clear breakdown on use of financial intelligence, interviews held with LEAs and case examples presented suggest that the financial intelligence is mostly used to pursue predicate offences and associated ML. Limited feedback is provided to the FAU on use of financial intelligence by LEAs. This practice does not enable the FAU to adequately assess the quality of its analysis and prioritise its own course of actions.

Although the legislative reforms and increased efforts in pursuing ML investigations represent a clear step forward, more investigative opportunities should proactively be undertaken and pursued by Czech law enforcement. The authorities succeeded to reach considerable number of ML convictions, including in some large scale ML cases, though the number of these was modest. Serious large scale third party and stand-alone ML investigations, prosecutions and convictions continue to be the exception. Focus of ML investigations and prosecutions is not fully in line with the central ML risks for the country in terms of underlying criminal activity. Dissuasive and proportionate sentences were obtained for ML.

Seizure and confiscation represent policy priorities for the Czech authorities. Recent improvements in the legislative and institutional framework (e.g. access to relevant databases and introduction of the 'extended confiscation'[1]) have already produced concrete results in

[1] Extended confiscation is a term used to reflect the ability to confiscate assets (in criminal proceedings) that go beyond the direct proceeds of a concrete criminal offence for which the defendant is prosecuted.

relation to freezing and seizure of assets. The amounts the Czech authorities confiscated and recovered during the period under review are significant. Nevertheless, these amounts are still far inferior to the sums seized and frozen. LEAs regularly carry out financial investigations in relation to proceeds-generating offences. There is an increasing specialisation in the area of financial investigation (at LEA and judicial levels) and external expertise is available upon request. However, little information was provided to demonstrate effective results with respect to undeclared cross border transportation of cash and bearer negotiable instruments. Data presented to the assessment team confirm that seizures and confiscation are largely related to the primary offences constituting ML risks.

During the final stages of the preparation of the NRA and since that time, a certain number of FT cases have been brought to light that confirm the realistic possibility of such activities taking place in the Czech Republic. The authorities have instituted programmes intended to mitigate these threats. Several investigations were launched in relation to the foreign terrorist fighters and other terrorism and FT related occurrences. One of these cases has reached the prosecution stage. Financial investigations are carried out in all terrorism related investigations, including at the pre-trial stage. One prosecution which was not technically for FT because the investigation originated from foreign intelligence rather than admissible evidence in court proceedings resulted in a number of convictions and significant sentences, demonstrating effective disruption of organised terrorism-FT activity and leading to the assessors' conviction that a "true" FT case would be dealt with in an effective and dissuasive manner.

The measures in place for application of UN targeted financial sanctions (TFS) related to both FT and proliferation financing (PF) are identical. As a member of the European Union (EU), the Czech Republic is negatively affected by the shortcomings identified in the EU legislation. This resulted in delays of implementation of targeted financial sanctions pursuant to relevant United Nations Security Council Resolutions (UNSCRs). To remedy this deficiency, the country introduced a national mechanism. This mechanism, although not requiring immediate freezing of assets but submission of a suspicious transactions report (STR) by a reporting entity, still ensures some elements of an effective system. The Czech Republic has no domestic mechanisms (apart from these developed under the EU framework) for implementation of the UNSCR 1373. Although the understanding among obliged entities on their obligations with respect to TFS varies considerably, there have been some false-positive matches identified with respect to FT and PF related designated persons and entities. In one case, the authorities succeeded to identify the assets of the entity which had links with the designated entity pursuant to UNSC Resolution 1718. Consequently, the authorities initiated a procedure for designation of that entity, which resulted in inclusion of the entity in the sanctions list.

The banks have an appropriate understanding of the ML/FT risks and obligations, but awareness is lower with the other financial institutions. The perception of the FT risks is based on the NRA, experience and/or group guidance, and guidance from the supervisors. Generally, all reporting entities demonstrated a good knowledge of the AML/CFT requirements, but the risk-based approach is applied mostly by banks, securities intermediaries and insurance industry. The quality of STRs increased significantly in the last couple of years. The banks are the main contributors in the overall volume of reports, while the number of STRs submitted by the designated non-financial businesses and professions (DNFBPs) is commensurate with their

The scope of the extended confiscation then goes to all the assets that are suspected to be proceeds of crime unless the defendant can prove their legal origin. The 'extended confiscation' notion is also included in the FATF Best Practices Paper on Confiscation (pg.6, par.17) whilst it became a part of the EU Directive 2014/42.

limited knowledge in the ML/FT area.

The Czech National Bank (CNB) has a robust financial institutions (FIs) licensing mechanism, including a sound process to make sure that criminals are not owners or managers of financial institution. On AML/CFT supervision, the FAU and CNB are the two main regulators that simultaneously oversee the biggest part of the financial sector. The efficiency of the existing model (duplication of duties for on-site AML/CFT supervision) might be an issue in a view of limited resources. The fines applied by the FAU and CNB are not playing their dissuasive and deterrent role and they are not applied in a proportionate manner.

The Public Register in the Czech Republic, include several registers: the Commercial Register, the Register of Associations, the Register of Foundations, the Register of Associations of Unit Owners and the Register of Benevolent Associations. Every public register can be accessed directly (on-line) and free of charge. Upon request, the authorities can require non-public information. LEA and Prosecution consider the Commercial Register as a good tool, which significantly improved since 2017. Trust and Beneficial Ownership Registers have been recently introduced but are still not fully populated with the respective data and information.

The Czech authorities have been active in relation to foreign requests, including those related to seizing and freezing assets. The feedback received from other jurisdictions was largely positive in terms of quality of mutual legal assistance (MLA) and did not highlight the timeliness as an issue of concern. The authorities also demonstrated significant activity with respect to the outgoing MLA requests across all predicate offences. The number of outgoing requests regarding ML offence also demonstrates that the authorities are proactive in seeking assistance from abroad. The relevant authorities (the FAU, LEAs, judiciary) proactively and constructively cooperates with their foreign counterparts by exchanging information on ML, associated predicate offences and FT, both spontaneously and upon request. Police and intelligence agencies are engaged in cooperative information sharing via different multi-agency platforms as well as in cooperation at the operational level (e.g. actively taking part in joint investigative teams).

Risks and General Situation

2. The Czech Republic is not a major international financial centre. The level of various forms of economic crime remains a key ML vulnerability of the country. The ML/FT National Risk Assessment recognised this fact and listed the following proceeds-generating offences, with subsequent money laundering and terrorist financing risks, as the most severe: various forms of tax crimes; corruption; public procurement (machinations); and subvention (or subsidies) fraud. Consequently, the most significant ML techniques include the abuse of services in the financial sector, in particular credit institutions and money remittance; misuse of advisory and legal professions and investment in real estate; abuse of betting accounts and services related to virtual currencies; and trade based money laundering. Terrorist financing, contrary to the other crimes listed, occurred to an extremely limited extent in the Czech Republic, and overall FT risk level may be summed up, at its highest, as “moderate”.

3. The banking sector is comprised of 45 banks. Out of the 45 banks, 23 are foreign bank branches. At the end of 2016, foreign owners controlled 93.1% of the assets of the Czech banking sectors (i.e. foreign bank subsidiaries or foreign bank branches), with 92.7% of the assets owned by foreign entities from EU Member States. In 2016, Czech banks directly managed CZK 5,960.9 billion (EUR 235.54 billion). With a 56.1% share, foreign currency loans and other receivables are the largest item of the foreign currency assets of the sector as a whole. A new fiscal responsibility framework was adopted in January 2017 which established, *inter alia*, an

independent fiscal council to assess compliance with the fiscal rules and evaluate the long-term sustainability of the public finances. Financial institutions and, in particular, banks and credit unions are exposed to an increased ML/FT risks in terms of customer numbers, quantity and volume of processed transactions. On the other hand, these financial institutions are the most active in taking their own risk mitigation measures and reporting suspicious transactions.

Overall Level of Effectiveness and Technical Compliance

4. Since the last evaluation, the Czech Republic has taken steps to improve the AML/CFT framework. AML/CFT Law was amended and these amendments entered into force as of 1 January 2017. The amendments require the authorities to, inter alia, conduct national risk assessment with a view of identifying ML/FT risks as well as to undertake measures to mitigate these risks. In relation to FT, amendments were introduced in the Criminal Code in February 2017. One of the most significant changes brought about by these amendments was introduction of a stand-alone provision on financing of terrorism, introduction of a terrorist group definition, explicit criminalisation of preparatory and ancillary conduct, support and promotion of terrorism, travelling for the purpose of terrorism, recruitment, training for terrorism, receiving training for terrorism and threatening with terrorism. Furthermore, criminal liability of legal entities has also been a subject of reforms. The relevant legislation now includes a 'negative list' enumerating criminal offences for which legal persons cannot be held criminally liable. Every other offence defined by the Criminal Code, may be therefore committed by a legal person, including money laundering and financing of terrorism.

5. To address the risks posed by complex corporate structures, starting 1 January 2018, the Register on Beneficial Owners and the Central Register of Bank Accounts were established to improve transparency of beneficial owners and to provide quicker access to bank account information.

6. The Czech authorities have achieved a substantial level of effectiveness in international cooperation; confiscation of proceeds and instrumentalities of crime; and FT investigations and prosecutions. Czech Republic has achieved moderate results in the other areas covered by the FATF standards.

Assessment of Risks, coordination and policy setting (Chapter 2 - IO.1; R.1, R.2, R.33)

7. The NRA was approved by the Government of Czech Republic in January 2017. The document addresses both ML and FT risks and includes assessment of threats, vulnerabilities and consequences. It also sets specific mitigating measures to address the risks identified. However, the majority of these measures have already been implemented or their implementation is underway, whilst future actions have rarely been introduced. The NRA also notes that, with respect to prevention and mitigation of ML/FT risks, the aim is to formulate a national AML/CFT strategy. At the time of the onsite visit, a unified national AML/CFT strategy had not yet been put in place.

8. The NRA process was driven by the in-house methodology based on FATF Guidance on National ML/FT Risk Assessment and was coordinated by the FAU. The process also involved other relevant authorities, self-regulatory bodies and the private sector. The NRA is reasonably comprehensive and it has clearly aided the understanding and knowledge of the competent authorities and the private sector on the ML/FT threats and vulnerabilities they face. Nonetheless, the classification of risks as per their importance appears not to be comprehensive enough - the heat map provided does include the ratings associated to different risks. The NRA identified tax crimes, fraud, corruption, phishing, and subvention frauds (otherwise be known as

"Subsidies Fraud", i.e. the abuse of government subsidies programs) as the most common predicate offences which trigger subsequent laundering of proceeds. FT, for example, was also under scrutiny due to its seriousness, whilst, on the other hand, it was concluded that the probability of its occurrence was low.

9. Following the approval of the NRA, the FAU prepared and disseminated to the reporting entities twelve non-public tailor made analyses of risks which correspond to specific segments of the private sector. The knowledge and understanding of AML/CFT risks by different reporting entities varies - whilst the financial institution demonstrated a relatively high level of understanding and awareness of ML/FT risks, the same cannot necessarily be stated for other reporting entities.

10. The lower risk scenarios for the application of simplified customer due diligence (CDD) measures are provided in the AML/CFT Law. The inherent risks corresponding to these exemptions do not stem from the NRA or other risk assessment. Authorities consider that the legal requirements for simplified CDD measures should be revised in order to correctly reflect the results of the NRA, and of the risk assessments carried-out by each obliged entity. Unlike the simplified CDD, the exemptions do result from the NRA, which revealed no or very limited exposure to ML/FT risks for the e-money and mobile payment services. With regard to enhanced measures, the AML/CFT Act does not explicitly require obliged entities to perform enhanced CDD (ECDD) where the ML/FT risks are higher. Thus, the NRA results do not directly support the application of enhanced measures for higher risk scenarios. It appears that the AML/CFT risk mitigation measures are taken based on clients' risk profile, including the application of ECDD in cases of "negative" information acquired from paid databases (e.g. WorldCheck) or from open sources.

11. Cooperation at operational level and information exchange between authorities is generally good, however certain improvements are needed with regard to monitoring of the implementation of the NRA Action Plan.

12. Following the NRA findings, the Czech National Bank assigned the supervisory activity to two of its departments – one which applies a comprehensive risk-based supervision system, and has a team dedicated solely to AML/CFT matters, and the other which includes AML/CFT issues as a part of its general supervisory activities. To address the risks posed by complex corporate structures, the Register on Beneficial Owners and the Central Register of Bank Accounts were also established.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.29-32)

13. The FAU has access (direct or indirect) to a broad range of databases containing financial, administrative and law enforcement information. It produces good quality financial intelligence, which is used to certain extent by the competent authorities to investigate ML and associated predicate offences. The results of FAU analysis are disseminated to the LEAs either in the form of a criminal complaint[2] or as information that they could use for the purposes of their pre-existing investigative activities. The FAU proactively seeks intelligence from the foreign counterparts to further support its financial intelligence analyses and investigations initiated by LEAs. The analytical capacities of the FAU allow them to carry out the analysis of complex cases and detect different sophisticated methods criminals use to conceal or disguise the origin of illegally

[2] Criminal complaint is a document/report (S. 159 CPC) that sets forth the basis upon which a criminal proceedings may be initiated. The standard is reasonable suspicion: person is to be charged with an offense.

obtained assets. In general, the intelligence gathered and criminal complaints submitted by the FAU correspond to the NRA findings on most common ML predicates indicated thereof. The coordination and cooperation between the competent authorities is smooth and prompt. However, limited feedback is provided to the FAU on the use of financial intelligence by LEAs. This practice does not enable the FAU to adequately assess the quality of its analysis and prioritise its own course of actions. LEAs also initiate ML investigations based on their own intelligence, complaints from the public and information gained in the course of investigating predicate offences. Cases of autonomous ML resulting from investigations initiated by LEAs are rather rare. The FAU is satisfied with the quality of STRs submitted by the obliged entities. As opposed to DNFBPs, the financial institutions submit the vast majority of STRs. While the NRA identified the real estate sector and legal professionals as vulnerable to ML abuse, only few STRs were submitted by these obliged entities. Close communication between the FAU and the obliged entities positively affects the suspicious transaction reporting. Some DNFBPs submit STRs to FAU through their respective self-regulatory bodies (SRBs). With this regard there are serious doubts with the function of these SRBs, since in practice, they, rather than the DNFBP concerned, make a decision whether the STR should be submitted. Deficiencies identified with respect to the definition of suspicious transactions, as well as the timeframe for submitting an STR may further hamper the proper compliance with the reporting obligations. The FAU has adequate human, financial and technical resources to conduct operational analysis. However no written guidelines on STRs prioritisation are in place. With regard to strategic analysis, apart from the typologies prepared for the purposes of the NRA, there is little evidence of the FAU's efforts hereof.

14. Most of the ML investigations and prosecutions stem from information gathered by law enforcement agencies and the FAU criminal complaints. The system and structure of the Czech criminal investigation and law enforcement arrangements gives the police the central and most active role in the pre-investigative and investigative stages. Police have at their disposal an extensive array of powers that are used fairly regularly for proceeds-generating offences. While it does appear that a considerable number of reports, suspicions or occurrences of ML result in the opening of a criminal proceeding, it does not necessarily follow that LEAs fully exploit the opportunities that are available to actively seek to identify evidence of ML in connection with the investigation of proceeds-generating predicates. Whilst the great majority of convictions relate to less sophisticated and less complex ML schemes, it was noted that Czech authorities do investigate on a regular basis ML cases where the predicate offence was committed abroad. The average time spent in pre-trial proceedings was 3.5 years, with the fastest time at 475 days and the slowest at 3189 days which seems too long. Prosecution authorities met on-site did express a certain amount of frustration at the length of proceedings under the current criminal procedure code. The data available for the vast majority of cases where convictions were obtained does not make it possible to establish a clear relationship with the higher risk areas. Consequently, it cannot be concluded that the ML investigations and prosecutions carried out fully correspond to the high-risk predicate profile of the Czech Republic. However, discussions with Czech authorities and examples provided do tend to confirm that this is the case, generally. The prevalent practice within the Czech justice system of sanctioning multiple offences simultaneously makes it difficult to measure the precise impact of the sentence in relation to ML. Nevertheless, in certain cases where ML was prosecuted in the absence of the predicate, dissuasive and proportionate sentences were obtained.

15. Strategic documents, the latest legislative changes together with the newly available tools and instruments confirm that the confiscation of the proceeds and instrumentalities of crime are given priority in the Czech Republic. The Czech Republic applies confiscation in criminal proceedings and also a specific form of administrative confiscation based on tax related

legislation. "Extended" confiscation and non-conviction based confiscation in criminal proceedings are in place as of 2017, but both have been applied only in some on-going cases. Since 2011, a total value of approximately CZK 8,68 billion (EUR 334 million) has been recovered. This amount is expected to increase significantly once the on-going complex investigations and proceedings, which included significant seizure of assets, are completed. Whilst the value of the confiscated assets is substantial, it is still far inferior to the sums seized and frozen. This appears to be a consequence of a lengthy pre-trial and trial proceedings and the fact that final convictions are yet to be achieved in numerous cases with significant confiscation requests. Although statistical breakdown on different types of confiscation of proceeds and instrumentalities including the property of equivalent value, confiscation from a third party, confiscation of fruits and revenues and confiscation of proceeds which have been moved abroad is not available, the cases presented to the assessment team confirm that all these elements are in place and regularly pursued by LEAs. As the Czech Republic has no external borders with non-EU countries, cash controls are applied only at 5 international airports. For the transportation of cash and bearer negotiable instruments the Czech Republic has introduced a declaration system in line with the EU control system. All imports and exports of cash or BNIs over EUR 10,000 on entry of the Czech territory from non-EU country must be declared in writing. Whenever a false declaration is made/undeclared cash is found, customs inform the FAU. If there are indications that cash is related to crime, including ML/FT, customs inform LEAs as well. However no statistical data were available on suspicious border incidents or on assets restrained due to the illegal transportation of currency and BNI. Although the NRA does not address the issue of confiscation in a comprehensive way, the statistics provided on types of offences where confiscation was applied confirm that the seizure/confiscation generally reflects the assessment of higher ML/FT risks.

Terrorist Financing and Financing Proliferation (Chapter 4 - IOs 9-11; R.5-8)

16. The NRA found, when considering FT risks, that the seriousness and consequences of this crime were quite "severe" and therefore the threat-level "high", but that their occurrence was infrequent and from this angle, the threat-level "low". Based on these findings, interviews held on-site and the foregoing considerations, the current FT risk level may be summed up, at its highest, as "moderate".

17. Regarding the prosecution of FT activities, at the time of the on-site visit one case was in the prosecution phase while ten investigations were still underway. Taking into account the terrorist-FT cases investigated and one being prosecuted (that touches upon the FT risk related to Islamic radicalism and to foreign terrorist fighters), there is evidence that the country's efforts are in line with the country's FT profile.

18. From 2015 the Police dealt with about 40 suspicions of FT yearly and these are investigated at least in a preliminary manner until a point is reached where the suspicions are found to have no real basis or, on the other hand, a decision is made to pursue the matter further. Both police and the FAU have the means to exchange information with the intelligence services and are equipped with knowledge and means to identify potential FT activity. Most cases never reached the prosecution stage but were closed once the investigation failed to discover sufficient evidence to demonstrate that the relevant criminal offence was in fact committed. The supervision of terrorist criminal offences and corresponding FT is performed by the High Public Prosecutor's Office in Prague. Terrorism financing is always a mandatory part of the investigation of each criminal case associated with terrorist criminal acts. In practice, investigation of a terrorism related offence includes a detailed analysis of bank accounts and transfers to or from the suspects (their financial 'activity') and creation of a financial profile of

the suspects. While summaries of several terrorism-related cases were shown to and discussed with the assessment team, the Czech authorities advised that they had not identified any facts clearly demonstrating occasions of conventional terrorist financing that can be proven based on admissible evidence. FT investigation is integrated, to some extent, with national counter terrorism strategies – in spite of the fragmentation of FT related elements into various strategic documents and lack of unified approach in targeting this matter.

19. Since there have not yet been any convictions for FT, there are no examples as yet of the application of sentences. There are examples, however, of dissuasive sentencing in relation to offences charged and prosecuted amidst allegations of FT, but where admissible evidence of FT could not be produced to a court.

20. The measures in place for application of UN TFS related to both FT and PF are identical. The Czech Republic applies the EU framework in relation to implementation of the UN TFS and thus is negatively affected by the shortcomings identified in the EU legislation. Consequently this results in delays of implementation of TFS pursuant to respective UNSCRs on FT and PF. With the aim to rectify these deficiencies, Czech Republic introduced a national mechanism. This mechanism, although not requiring immediate freezing of assets but submission of a STR by a reporting entity, still ensures some elements of an effective system. Shortcomings are identified in relation to communication of designations at a national level. Apart from larger financial institutions, there is no clear understanding among other obliged entities on their freezing obligations. These obliged entities consider that where there is a match with a designated person or an entity, their only obligation is to contact the FAU for further instructions. The Czech Republic has no domestic mechanisms (apart from these developed under the EU framework) for implementation of the UNSCR 1373. The risk of NPOs' exposure to FT was assessed based only on some hypothetical examples of FT abuse. Hence, the subset of NPOs actually falling under the definition as stipulated under FATF Recommendations has not been identified. The outcomes of the NRA have not been sufficiently discussed with the NPOs, and their representatives interviewed on-site were unaware of the potential typologies of NPO's abuse. Measures taken by the authorities with respect to prevention of terrorism related persons and entities from raising, moving and using funds and abusing the NPO sector, are consistent with the Czech Republic FT risk profile only to some extent. The Czech Republic has yet to put in place a risk-based system for targeted monitoring of its NPO sector.

21. Little is being done to detect funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities. Nevertheless there have been some false-positive matches identified both on FT and PF, which demonstrates some effectiveness of the system in place. However, technical deficiencies related to the freezing of funds and other assets of terrorist-related persons without delay, definition of funds to be frozen, as well as deficiencies identified with regard to the timeliness of suspicious transactions reporting (STR) and the role of self-regulatory bodies in the STR process have further negative impact on the effectiveness. Whilst the country did not initiate listing/de-listing with regard to terrorism financing TFS during the period under review, in one case, the authorities demonstrated effective co-operation and co-ordination leading to identification of assets of an entity which had links with the designated entity for proliferation financing. The Czech authorities also initiated the procedure for designation of that entity, which was subsequently approved by the UNSC Committee established pursuant to Resolution 1718.

22. Supervision on implementation of TFS forms a part of each inspection conducted in financial institutions. However, sanctions applied do not seem proportionate and dissuasive. Limited training on PF has been provided to the reporting entities. Although the CNB developed a guidance on procedures for implementation of the UNSCRs by the financial institutions, the

representatives of these institutions interviewed on-site were not aware of it. No guidance was developed for other obliged entities.

Preventive Measures (Chapter 5 - IO4; R.9-23)

23. The financial institutions appear to have a good knowledge of their AML/CFT obligations and have a constructive relationship with both the FAU and other supervisors. The banking sector demonstrated a proactive approach to risks and good understanding of their AML/CFT obligations. Banks do not use the Czech NRA as the unique source for their risk analysis, but also consider the EU Supra-National Risk Assessment, public sources, their own experience, and group-wide assessments. The understanding of AML/CFT risks, and the acceptance of the NRA findings amongst the DNFBPs varies, but they rarely apply a risk-based approach to their AML/CFT measures.

24. The private sector is aware that enhanced measures must be taken in the areas of increased risks. The on-going monitoring regime is employed based on the customer's risk profile. In most of the cases, the banks perform automatic screening of their existing customers to adjust their classification. Risk-based decisions are taken by a number of financial intermediaries to restrict or exclude some business lines according to the risk appetite set in the AML/CFT internal rules. Less attention appears to be paid by some non-banking financial institutions to the identification of politically exposed persons (PEPs).

25. Financial institutions are generally familiar with their CDD and record keeping responsibilities. In the verification process, the banks have access to several public and restricted databases. However, the access to the databases held by the Czech authorities is an area for improvement. The issue of verification of beneficial owners persists to a large extent.

26. The STR regime is largely in place with the banks being the main contributors in terms of STR submission. While the evaluators admit that contextually the highest volume of financial assets and financial transactions are held/performed by the banks, there are sectors where the ML/FT risks remain present, without this being reflected in the reporting behavior.

27. AML/CFT systems in all credit institutions, life insurance companies and pension companies are subject of independent internal audits without any specification regarding the periodicity. The financial institutions include the AML/CFT issues into their internal audit plans on the basis of their own risk assessments.

Supervision (Chapter 6 - IO3; R.26-28, R. 34-35)

28. The CNB has a robust FIs licensing mechanism, including a sound process to make sure that criminals are not owners or managers of financial institution. Some deficiencies have been identified in relation to the ability to recognize PEPs and associates of criminals in the authorisation process. The AML/CFT Chief Compliance Officers of credit institutions are not subject to any mandatory qualification requirements or "fit and proper" tests. For gambling business, the basic license is issued by the Ministry of Finance, which verifies the provided data using publicly available sources. The real estate agents, accountants, trust and company service providers, dealers in precious metals and stones and traders in items of cultural heritage or items of cultural value are not subject to licensing.

29. The FAU and the CNB have a good understanding of ML/FT risks. The two main supervisors demonstrated significant efforts in promoting the results of the risk assessment amongst the entities under their remit. On a less positive side, both the FAU and the CNB have

very limited human resources responsible for AML/CFT supervision. The representatives of the professional Chambers demonstrated a satisfactory level of understanding of AML/CFT risks.

30. CNB`s Financial Market Supervision Department applies a comprehensive AML/CFT risk-based supervision system (RAS/RAS II) which is to a lesser extent implemented by the CNB Financial Market Supervision Department II. The model used by the FAU to determine the frequency and depth of on-site audits does not consider individual institution risk or risks assigned for groups of institutions within particular sectors. The criteria used by professional Chambers for inspections planning do not contain specific ML/FT components.

31. Pecuniary sanctions applied by the FAU and the CNB are not playing their deterrent role and they are not applied in a proportionate manner. Although the remedial measures have a positive impact, in the absence of dissuasive fines, sustainable and effective self-compliance efforts by the FIs are not ensured. Supervision by Professional Chambers is not at the stage where it can prove an impact on AML/CFT compliance by legal professions.

32. The FAU and CNB continuously perform significant efforts in promoting a clear understanding of AML/CTF obligations and ML/FT risks amongst reporting entities (Res).

Transparency of Legal Persons and Arrangements (Chapter 7 - IO5; R. 24-25)

33. The existing Public Registrar and yet not fully populated Registrars of Beneficial Ownerships (BOs) and Trusts constitute a positive move towards a transparent and open culture in respect of legal persons and arrangements. Whilst, at the moment, information on legal persons is publicly available and can be obtained from the Public Registrar, the Registry of Trusts and of the BOs will only be entirely operational by the end of 2018 (trusts) and by the end of 2021 (BOs).

34. The NRA reviews the risks associated with a few types of legal entities, and provides some typologies of abuse of the entities. However, the vulnerabilities related to different ownership structure of legal persons are not comprehensively reviewed, and the risk associated with foreign entities is not considered.

35. All types of legal persons established under private law are obliged to register in the Public Register in the Czech Republic. The law enforcement authorities maintained that the quality and accuracy of the registry data have improved significantly in the last years. The Court does not have an authority or obligation to verify the correctness of the information provided, but the assessment team positively notes that the City of Prague Registry Court appointed three judges to dissolve inactive companies. This measure already bore fruits and significantly contributed to an increased accuracy and reliability of the database.

36. All existing public registers can be accessed directly and free of charge through the internet and, upon request, the public authorities can require non-public information (such as copies of the documents) which is provided in a timely fashion.

International Cooperation (Chapter 8 - IO2; R. 36-40)

37. The Czech Republic has comprehensive legal framework for the MLA and extradition, which enables the authorities to provide the widest possible range of assistance in relation to investigations, prosecutions and related proceedings concerning ML, associated predicate offences and FT. Over the last few years Czech authorities have maintained a high level of activity in relation to incoming requests for MLA based on all offences that have been received in increasing numbers. Feedback received from other jurisdictions about the promptness and general quality of the assistance provided by Czech authorities is quite positive in general.

Partial statistics are available in relation to outgoing MLA requests related to ML and certain predicates, therefore it is difficult to conclude that these requests properly respond to the need to seek assistance in accordance with the Czech Republic's risk profile. Still there is an adequate number of requests pertaining to ML. Regarding extradition several examples presented to the assessment team touched upon drugs and embezzlement, which are high-risk offences for the Czech Republic. The supervisory authorities can exchange information with their foreign counterparts from EU and non-EU countries, including the information held by the financial institutions. CNB cooperates intensively with its foreign counterparts and this cooperation also includes on-site inspections at the requests of the foreign counterparts. The FAU and LEAs proactively and constructively cooperate with their foreign counterparts by exchanging information on ML, associated predicate offences and FT, both spontaneously and upon request. Police and intelligence agencies are engaged in continual cooperation with their foreign counterparts. This includes cooperative information sharing via different multi-agency platforms as well as cooperation at the operational level (e.g. actively taking part in joint investigative teams). Czech authorities provided cooperation, via MLA, regarding beneficial ownership of legal persons and arrangements within a reasonable time period. Such cooperation will presumably be more and more prompt as the newly created Czech Beneficial Ownership Register is adequately populated.

Priority Actions

- Update the NRA so that it clearly indicates the ML and FT risk levels associated to different risk areas. Update the Chapter 4.1 of the NRA, revise the measures included therein, focus more on the actions which resulted from the analysis of risks and specify their intended outcomes in order to allow for proper monitoring of their implementation.
- LEAs should use the financial intelligence provided by the FAU more proactively to investigate ML cases independently and not only when targeting the underlying criminal activity. LEAs should regularly provide detailed and adequate feedback to the FAU on the quality of their dissemination and their further use, indicating the type of criminal activity information is used for.
- Czech authorities should focus more efforts and, as required devote greater resources to large scale and complex ML prosecutions that more closely align with the identified risk predicates; the authorities should find ways, including as required through legislative amendment, to streamline the pre-trial process in order to shorten the average length of prosecutions in serious ML cases.
- The authorities should carry out periodically a stock taking exercise on effectiveness and impact of the recently introduced non-conviction based confiscation (NBC) and extended confiscation mechanisms. Based on the results of these periodic exercises the appropriate measures should be included in the updated NRA and Strategy to Combat Organised Crime; the capacities of the relevant authorities in the area of cross-border control of cash and BNI should be strengthened whilst LEAs should be given a mechanism to freeze the cash whose origin is unknown.
- Czech Republic intelligence services, the FAU and police authorities should ensure that they stay in step with the changing landscape in relation to FT by maintaining close contacts with foreign counterparts; the authorities should clearly establish, and, as appropriate continually re-evaluate, the risk level for FT and inform reporting entities accordingly.

- The authorities should ensure that the implementation of UN TFS on FT and PF is without delay enabling a prompt application of freezing measures for the duration of the validity of an action initiated by the UNSCRs.
- The authorities should revise or conduct a new in-depth risk assessment of the NPO sector to identify those that are at risk for FT abuse. In addition, targeted and coordinated risk based approach in monitoring higher risk NPOs, should be implemented.
- The authorities should intensify and enrich the trainings provided to non-banking financial institutions (especially payment service providers and currency exchangers) and DNFBPs on ML/FT risks and respective mitigating measures to further clarify that the DNFBPs should assess their entity wide risks, risks arising from their products and customers. When assessing the risk the NRA, relevant guidance, typologies and feedback from the FAU should be taken into account.
- The authorities should improve the licensing procedures for financial institutions and DNFBPs so that includes: (a) processes of verification of legitimate source of funds; (b) take measures to prevent criminals and their associates from being professionally accredited or holding a significant or controlling interest, or a management function in all DNFBPs; (c) take measures to ensure that their managers, UBOs or controllers are not the associates of criminals.
- The sanctioning regime should be enhanced by: applying dissuasive and proportional pecuniary sanctions to financial institutions and DNFBPs, and by clearly identify the management positions that can be sanctioned for AML/CFT breaches.
- The authorities should carry out a comprehensive analysis of risks associated with all types of legal entities. Measures should be in place to enable the registrars of basic and beneficial ownership information to be able to verify whether information provided to them is adequate, accurate and current; this framework should be actively implemented by the registrars.
- Authorities responsible for MLA and Extradition should establish more complete systems for tracking the number and nature and delay in relation to their cases, particularly in respect of ML matters and their predicates.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings

IO.1 – Risk, policy and coordination	IO.2 – International cooperation	IO.3 – Supervision	IO.4 – Preventive measures	IO.5 – Legal persons and arrangements	IO.6 – Financial intelligence
Moderate	**Substantial**	**Moderate**	**Moderate**	**Moderate**	**Moderate**
IO.7 – ML investigation & prosecution	IO.8 – Confiscation	IO.9 – TF investigation & prosecution	IO.10 – TF preventive measures & financial sanctions	IO.11 – PF financial sanctions	
Moderate	**Substantial**	**Substantial**	**Moderate**	**Moderate**	

Technical Compliance Ratings (C – compliant, LC – largely compliant, PC – partially compliant, NC – non compliant, N/A – not applicable)

R.1 – assessing risk & applying risk-based approach	R.2 – national cooperation and coordination	R.3 – money laundering offence	R.4 – confiscation & provisional measures	R.5 – terrorist financing offence	R.6 – targeted financial sanctions – terrorism & terrorist financing
LC	**PC**	**LC**	**C**	**LC**	**PC**
R.7 - targeted financial sanctions – proliferation	R.8 – non-profit organisations	R.9 – financial institution secrecy laws	R.10 – Customer due diligence	R.11 – Record keeping	R.12 – Politically exposed persons
PC	**PC**	**C**	**LC**	**LC**	**LC**
R.13 – Correspondent banking	R.14 – Money or value transfer services	R.15 – New technologies	R.16 – Wire transfers	R.17 – Reliance on third parties	R.18 – Internal controls and foreign branches and subsidiaries
PC	**C**	**LC**	**LC**	**LC**	**LC**
R.19 – Higher-risk countries	R.20 – Reporting of suspicious transactions	R.21 – Tipping-off and confidentiality	R.22 - DNFBPs: Customer due diligence	R.23 – DNFBPs: Other measures	R.24 – Transparency & BO of legal persons
PC	**PC**	**PC**	**PC**	**PC**	**LC**
R.25 - Transparency & BO of legal arrangements	R.26 – Regulation and supervision of financial institutions	R.27 – Powers of supervision	R.28 – Regulation and supervision of DNFBPs	R.29 – Financial intelligence units	R.30 – Responsibilities of law enforcement and investigative authorities
LC	**LC**	**LC**	**LC**	**LC**	**LC**
R.31 – Powers of law enforcement and investigative authorities	R.32 – Cash couriers	R.33 – Statistics	R.34 – Guidance and feedback	R.35 – Sanctions	R.36 – International instruments
C	**PC**	**PC**	**LC**	**PC**	**LC**
R.37 – Mutual legal assistance	R.38 – Mutual legal assistance: freezing and confiscation	R.39 – Extradition	R.40 – Other forms of international cooperation		
LC	**LC**	**LC**	**LC**		

MUTUAL EVALUATION REPORT

Preface

1. This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

2. This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 5 to 16 March 2018.

3. The evaluation was conducted by an assessment team consisting of:

Mr Claude LEFRANCOIS, Senior Counsel, International Assistance Group, Litigation Branch, Department of Justice Canada (legal evaluator);

Ms Magdalena SOCHACKA, Police Officer, National Police Headquarter, Poland (legal evaluator);

Ms Ani GOYUNYAN, International Relations Specialist, Financial Monitoring Center, Central Bank of Armenia (law enforcement evaluator)

Mr George NIKOLAISHVILI, Chief Specialist at Analytical Department, Financial Monitoring Service of Georgia (financial evaluator), and

Mr Igor BEREZA, Director, AML/CFT Department, National Bank of Ukraine (financial evaluator)

with the support from the MONEYVAL Secretariat:

Mr Lado Lalicic, Head of AML/CFT Monitoring, Typologies and Conference of the Parties to CETS no. 198 Unit;

Ms Irina Talianu, Administrator, and

Ms Ani Melkonyan, Administrator.

The report was reviewed by the FATF Secretariat, Mr Carmine Carrella (Italy) and Mr Tomislav Sertic (Croatia).

4. Czech Republic previously underwent a MONEYVAL Mutual Evaluation in 2010, conducted according to the 2004 FATF Methodology. The 2011 evaluation report has been published and is available at https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680715f78.

5. That Mutual Evaluation concluded that the country was compliant with 4 Recommendations; largely compliant with 21; partially compliant with 22 whilst no Recommendation was rated non-compliant. Two Recommendations were considered to be non-applicable. The Czech Republic was rated compliant or largely compliant with 10 of the 16 Core and Key Recommendations.

6. The Czech Republic was placed under regular follow up immediately after the adoption of its 4th Round MER. As of September 2015, the Czech Republic was placed under MONEYVAL Compliance Enhancing Procedures, most notably due to continuous lack of progress on remedying gaps in money-laundering (former R.1) and terrorist financing (former SR.II) offences. In December 2016, the MONEYVAL Plenary, in line with its Rules of Procedure, suspended the CEPs since the onsite visit for the Czech Republic in the 5th round of mutual evaluations was scheduled for the first half of 2018.

CHAPTER 1. ML/TF RISKS AND CONTEXT

7. The Czech Republic (CzR) has a territory of 78.703 km^2 and a population of 10.56 million (World Bank, 2016). It is a landlocked country situated in Central Europe, bordering Poland, Germany, Austria and Slovakia. The capital of the Czech Republic is Prague, which is, with 1.259 million inhabitants (2015 UN data) also the largest city in the country. In 2016, the gross domestic product (GDP) of the Czech Republic was USD 195.31 billion (EUR 157.94 billion).

8. The Czech Republic is a parliamentary republic, with the power divided into legislative (Czech Parliament), executive (Czech Government and the President of the Republic) and judiciary. The Parliament is bicameral, made up of the House of Parliament and the Senate. The House of Parliament, based on the principles of proportionate representation, is re-elected every four years and consists of 200 members. The government is established on the basis of the outcomes of these elections. The Senate organises elections every two years, in which one-third of the senators is elected. In total, the Senate counts 81 members. Its main functions are to establish conditions for a quality legislative process and to ensure Parliamentary continuity in the event that the House of Parliament is dissolved. The Czech Government is the supreme body of executive power; the President of the Republic is the head of state and the supreme commander of the armed forces. The President is elected through presidential elections. The court system is made up of the Supreme Court; Supreme Administrative Court; Regional and District Courts. The Constitutional Court, made up of 15 judges serving for a 10-year term, oversees adherence to the Czech constitution.

9. The Czech Republic joined the Council of Europe (CoE) as the 35rd Member State in 1993. Since 2004 the country is a member of the European Union (EU), although it has not introduced the Euro as its official currency. The Czech crown is not subject to any IMF exchange floor, but the Czech National Bank in 2016 continued to implement its monetary policy in an environment of "technical zero" interest rates and under a temporary exchange rate commitment at CZK 27 to the euro. However, in April 2017, the CNB removed the koruna-euro floor. Apart from the CoE and EU, the Czech Republic is a member of other internationally and regionally relevant international organisations, such as the United Nations (UN), the North Atlantic Treaty Organisation (NATO), the Organisation for Security and Cooperation in Europe (OSCE), the World Trade Organisation (WTO), the European Bank for Reconstruction and Development (EBRD), the International Monetary Fund (IMF/WB), the Organisation for Economic Co-operation and Development (OECD), the Visegrad Group, Europol and Interpol.

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

10. The Czech Republic is not a major international financial centre. The Basel Institute AML Index 2017 places the Czech Republic on the 126th rank out of 156 with a score of 4,57 (the first position scores 8,6 with the highest ML risk, and the last position with a score of 3,04 presents the lowest risk as calculated by using this methodology). Transparency International has ranked the Czech Republic in 42nd place out of 180 countries in their corruption perception index. The country scores 57, where a score of 0 indicates a highly corrupt country whereas 100 indicates no corruption risk.

11. The Czech Republic finalised its work on a national risk assessment (NRA) in 2016. It lists the following proceeds-generating offences with subsequent money laundering and terrorist

financing as the most severe: various forms of tax crimes; corruption; public procurement (machinations); and subvention (or subsidies) fraud. Terrorist financing, contrary to the other crimes listed, occurred to an extremely limited extent in the Czech Republic, but the authorities consider and investigate this crime with the highest priority given its potential consequences to the society and its core values. Although rated less severe, drug crime and fraud + phishing are listed as the most frequent offences.

12. Entities which are considered most vulnerable for misuse by ML/FT threats, among financial institutions are those banks which have a low level of compliance (the NRA clearly states that only few banks with lower level of compliance were identified) and credit unions; whilst among DNFBPs these are tax advisors, lawyers and public notaries.

13. Corruption persists to be one of the problems in the Czech Republic. During the Panama Papers scandal that emerged in April 2016, of the 11 million documents released, over 250.000 had a connection to the Czech Republic. Nearly 300 Czech business figures appeared in the files. Many of the cases involved alleged tax evasion or money laundering.

ML Threats

14. The NRA indicates that methods of money laundering are continuously developing. The most significant techniques are the abuse of services in the financial sector, in particular credit institutions and money remittance; misuse of services of obliged entities in the non-financial sector, in particular advisory and legal professions and investment in real estate; misuse of services provided by other than obliged entities under the AML Act, e.g. abuse of betting accounts and services related to virtual currencies[3]; and trade based money laundering. The NRA categorises these threats as high. Conversely, laundering of foreign money is indicated as a low risk.

15. The NRA indicates an insufficient knowledge on the part of some of the obliged entities on ML/FT related risks and their management, as well as insufficient supervision of AML/CFT measures applied in practice by legal professionals. Measures that the NRA foresees to improve the system include both legislative and non-legislative. Particularly relevant are those which are likely to improve awareness-raising on AML/CFT prevention and those aimed at strengthening the supervision and reporting frameworks introduced towards de-risking of ML/FT.

16. The legal framework appears to have no constrains for financial investigations to be put in place whenever a proceeds generating offence(s) is committed. Financial investigation leads to the creation of complete financial profile of the perpetrator(s). Investigators identify assets that can be seized taking into account both, the direct proceeds of crime and/or a substitute value for a damage caused by the crime. Financial investigation is conducted simultaneous with the investigation of the predicate offence.

17. The experience gained through financial investigations suggests that persons with secondary and tertiary education predominate among the suspects and accused for proceeds generating crimes. In general, for the economic crime related activities, organised groups with a hierarchical arrangement and division of functions prevail. These groups involve foreigners as managers of companies with some form of legal residence in the Czech Republic. Moreover, lawyers, public notaries and tax advisers are increasingly involved in fraudulent business. Also white collar crime and third party money laundering (ML/FT techniques used in turnkey legalisation) are part of an increasing trend of financial crimes.

[3] Virtual currencies are covered by the AML/CFT Act as of January 2018 – as a result of application of one of the mitigating measures foreseen by the NRA Action Plan.

TF threats

18. Although the Czech Republic does not have direct experience with terrorist attacks, the threat of FT is perceived as very serious by all authorities concerned. Based on both - the National Risk Assessment and the National Security Audit that were carried out by the authorities, the current FT risk level may be summed up, at its highest, as "moderate". Financing may come from legal activities, such as charity funding or businesses, but also from illegal sources such as underlying criminal activities. Funds which draw the authorities' attention are mostly those collected through social solidarity and charity actions; through abuse of social benefits; or proceeds from illegal activities such as arms trafficking, drugs, illegal migration and extortion.

19. The NRA makes note of the risk of FT and transfer of funds for the purpose of FT through the use of cash couriers. Courier detection is more difficult as the Czech Republic is a part of the Schengen area. As far as the so-called *hawala system is concerned*, in the Czech Republic such activity would be considered illegal and prosecuted as per Section 251 of the CC. However, no such case has been identified. Another risk is posed by the vulnerability of NPOs, which could be abused for FT purposes.

20. The Czech Republic also finds threats coming from the so-called Islamic State (ISIL), including its foreign terrorist fighters (FTFs) and their funding. External funding sources for ISIL can come from funds gathered by FTFs, and funds gained from media and social network campaigns. The NRA has listed a number of possible risk factors and suspicious indicators with regard to potential ISIL and FTFs financing. The country has experienced only minor and rare cases of home-grown Islamic radicalism. However, in 2016 there was one case in which a native Czech citizen attempted to travel to Syria to join ISIL. Moreover, the Czech counter-intelligence agency (Security Information Service, BIS) reported one case in which money was transferred to a terrorist group.

21. In one case of FT investigated by the Czech Republic, Germany and Bulgaria, several co-conspirators were suspected of involvement in the procurement of funds, the acquisition of false personal and travel documents and the recruitment of fighters for an organisation which aimed to create a state in the form of an emirate or caliphate. The Czech Republic was mainly used as a transfer state for documents and finances, but Czech documents were also used to conclude short-term loans that were sent as contributions to comrades. During the house searches, a number of illegal materials such as personal documents, weapons and counterfeit banknotes were found and seized. It appeared the fight was aiming for a "liberation struggle" in the Caucasus. The link to terrorism financing (established through foreign intelligence) could not be confirmed through admissible evidence, but the suspects were prosecuted, convicted and firmly sentenced for their actions based on more "traditional" offences.

ML/FT vulnerabilities

22. The most prominent threat identified in the Czech ML/FT risk assessment, in terms of its consequences, is, in particular, the tax crime and related laundering techniques, followed by other underlying criminal offenses, such as corruption. An extremely serious threat, although, at the moment, with very low occurrence, is the financing of terrorism. Fraud, phishing and subsequent laundering techniques are very likely to occur.

23. The NRA "heat map" also refers to the following key areas: risks posed by trusts, insufficient awareness of risks by some DNFBPs in conjunction with insufficient supervision over their AML/CFT obligations, the use of cash, risks posed by corruption in both the public and private sectors, the low number of convictions for ML, risks posed by insufficient criminalisation of the FT offence, insufficient transparency and risks of abuse of NPOs for FT.

24. The Czech political arena witnessed a series of corruption scandals in recent years. Most notably, in 2013, the Prime Minister resigned after prosecutors charged his Chief of Staff with corruption and abuse of power, whilst in June 2017 the Czech parliament voted to strip the immunity of the leading candidate for next Prime Minister, so that he could be prosecuted for allegedly manipulating ownership of a subsidiary of a conglomerate, and thus illegally obtaining 1.91 million Euros from the EU. In September 2017 the Czech branch of Transparency International published a list of Czech politicians who have been lobbying for the Azerbaijani regime in the so-called "Laundromat". The connections of the foreign politicians with investments in the Czech Republic were the subject of interest within the Organised Crime and Corruption Reporting Project in 2012. This investigative reporting platform linked significant investments in the Czech Republic with the important political figures from Azerbaijan.

25. The highest degree of residual vulnerability (high exposure to threats in relation to the low level of currently enforced measures) among obliged entities is within the legal and advisory professions as well as with some gambling operators.

26. The efficiency of the Czech criminal justice system does not seem to be a major concern. However, the Czech branch of Transparency International raises concerns about prosecutorial independence. The 4th Round MER revealed a lack of reliable statistics and information on the performance of law enforcement and the judiciary in money laundering investigations, prosecutions and convictions, as well as in respect of execution of confiscation orders.

27. As already noted, the NRA also lists the mitigating measures to be taken in the areas of prevention, analysis, investigation and prosecution. These measures include the strengthening of the ML/FT risk management in particularly vulnerable sectors; introduction of measures to effectively prosecute ML; introduction of an electronic case management system in the prosecution service; systematic revision of certain provisions of the Czech AML Act in the light of a dynamic risk-based approach; and the full implementation of the FATF Recommendation 8.

Country's risk assessment

28. Czech Republic's NRA was adopted in January 2017 using the *FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment*. The NRA exercise brought together a wide range of authorities, FIs and DNFBPs. The FAU was co-ordinator of the overall process of carrying out the NRA. The NRA provides a detailed assessment of threats and vulnerabilities.

Scoping of higher risk issues

29. The assessment team identified those areas which required an increased focus through an analysis of information provided by the authorities, including the NRA, and by consulting various open sources.

a. Legal, operational and institutional issues

30. **Criminalisation** As of September 2015, the Czech Republic was placed under the MONEYVAL Compliance Enhancing Procedure (CEP), most notably due to continuous lack of progress on remedying gaps in the criminalisation of money laundering (former R.1) and terrorist financing (former SR.II). Whilst the latter offence was the subject of the Criminal Code reform in late 2016, legalisation of the former, when read in conjunction with the recent sources of interpretation, overall does criminalise sufficiently the required specific acts that constitute ML in accordance with the standards. The assessment team therefore dedicated increased attention to the impact of this situation on the effective application of the AML/CFT framework in practice.

31. **Money laundering.** The NRA identified a number of techniques used by the launderers. The document stated that the laundering process is carried out by a "*layer of wealthy*

entrepreneurs who at first sight do not show characteristic of a criminal; on the contrary, they act in public life as respected citizens, employing sophisticated techniques of committing mainly economic and property crimes. Various consultants such as lawyers, charted accountants, tax advisors, IT specialists provide them with complete know-how in the decision-making process, pertaining to both their criminal activities and legal business". In light of the foregoing the evaluation team examined tools and mechanisms the authorities use to identify illegal money flows. Further ML typologies have been analysed in conjunction with the findings of the NRA and the risk-based approach applied by the obliged entities. Last but not least, the assessment team has focused on the reasons for the low number of ML convictions.

32. **Terrorism financing.** The NRA did not provide a "one-word" or unique rating of the FT risk. The National Security Audit (NSA) assessed the FT threat level (as opposed to the risk level) as "medium". The country has experienced only insignificant cases of home-grown Islamic radicalism. One case is known in which a Czech citizen attempted to travel to Syria to join IS; another case involved a local imam who allegedly (the matter is currently being prosecuted) provided support and encouraged a couple who travelled to the conflict zone and joined ISIL. The evaluation team verified whether the Czech Republic had assessed FT risks in line with the current global and regional threats, including in relation to the NPO sector and FATF Recommendation 8 requirements. The evaluation team also considered whether the NPO sector understands their risk of being abused for FT purposes, and the extent to which authorities have conducted an outreach to NPOs.

Most common predicate criminality

Corruption, fraud and tax crimes

33. Corruption and various types of fraud and tax crimes are significant proceeds generating crimes. The assessment team particularly looked into the extent to which the effectiveness of the criminal justice system and the AML/CFT supervisory framework had been compromised at times by corruption. It also assessed the level of effectiveness in investigating and prosecuting ML, particularly when corruption and fraud appear as predicate offences. It considered the recent reforms that focused on law enforcement authorities and their potential for increased co-operation and co-ordination. Special consideration was given to the extent to which parallel financial investigations are used to trace, seize and confiscate the proceeds of crime. The assessment team sought to identify challenges faced by law enforcement when building the cases, their subsequent examination before the courts, and the level of evidence needed to achieve convictions and confiscations. Lastly, the average timeframe of ML cases (from identification to conviction) was another area for examination including *modus operandi* applied by the FAU and LEAs when identifying and prioritising investigations triggered by STRs.

34. To fight high-level corruption from a national point of view, the Council of Europe Group of States against Corruption (GRECO) recommended reforms aimed at increasing transparency of the legislative process, as an appropriate measure in the absence of regulations on lobbying. The evaluation team considered how the interaction with third parties seeking influence in the legislative process as well as the overall transparency with regard to national lobbying, constitutes a potential vulnerability of the AML system.

Drugs and human trafficking

35. According to the UN and OSCE reports, the Czech Republic is a country of origin, transit zone and a country of destination for victims of human trafficking. Victims mostly originate from Eastern Europe (particularly Ukraine), and East and South Asia and West Africa. With regard to drug trafficking, a considerable growth in seizures of various narcotics has been noted in recent years. The NRA does not specify the exact drug trafficking patterns which generate the proceeds

in Czech Republic. The evaluation team therefore assessed whether the measures in place to fight ML related to drug and human trafficking are effective, discussed the possible challenges that prosecutors may face in relation to the investigation and prosecution of these offences including the subsequent laundering and confiscation of proceeds derived therefrom.

36. **Beneficial ownership.** The assessment team reviewed the effectiveness of the beneficial ownership (BO) registration system in determining the extent to which it captures full, accurate and current BO information. It also explored the extent to which information on the identity of owners and other stakeholders as well as accounting information on the transactions carried out by foreign entities and other organisational structures is accurate and accessible. The recent reforms resulting in setting up of the central BO Register were also assessed in the course of the on-site visit.

37. **CDD verification process**. The NRA stated that the credit institutions operating in the Czech Republic successfully apply a risk-based approach, although certain vulnerabilities were noted, whereas the MONEYVAL 4th round MER noted certain deficiencies in the CDD processes. The evaluation team looked into the process of CDD, to determine the extent to which BOs information is identified, verified and analysed. It also considered whether money remittance services, the bureau de change sector, and legal and advisory professions and trusts and service providers faced the greatest exposure to ML/FT risks, as the NRA stated.

Regulation and supervision

Supervision of Financial Institutions (FIs)

38. The IMF identified gaps in the requirements for preventing banks from being used for criminal activity[4]. A general lack of resources for supervision of financial institutions raised particular concern. The evaluation team looked into the supervisory regime to appraise the effectiveness of the supervision process and the overall level of financial institutions' compliance with AML/CFT obligations. Resources available to apply sanctions and conduct AML/CFT inspections were considered.

DNFBP supervision and sanctioning

39. The 4th round MER identified deficiencies with regard to ML sanctions for DNFBPs, as well as a lack of result-sharing between the professional chambers of lawyers and the FIU. The evaluation team considered the extent to which failure to apply the AML/CFT regulations have been observed within DNFBPs and the remediation measures are taken in this regard. Moreover, it focused on the efficiency of co-ordination of supervision between the professional chambers and the FAU.

NPO regulation and supervision

40. In 2011 a lack of control on the legal entities that perform as non-profit organisations was identified, especially of high-risk entities. Moreover, the NPO noted the fact that the risk of abuse of NPOs to support and fund terrorism had been considered by the authorities, but yet not fully determined. Authorities noted that the proper implementation of R.8 is important and that, based on the issues arising from these considerations, a number of mitigating measures had been identified, many of which were already implemented or their implementation underway. For these reasons, the assessment team considered whether the Czech Republic installed a system that provides for sufficient targeted supervision or monitoring of NPOs that control a significant portion of the sector's financial resources, and play a substantial role in international

[4] IMF, 'Financial Sector Assessment Program report' (2012).

activities. It also focused on the evaluation and understanding of risks by competent authorities as well as on the effectiveness of measures deployed thus far against the actual risks posed by NPOs.

41. **Financial Intelligence Office.** In January 2017, the Czech FIU changed its status from a Department within the Ministry of Finance to an independent administrative office under the same ministry (FAU). The evaluation team analysed how this structural change influenced the independence of the FIU, the effectiveness of the analytical work and the domestic and international co-operation. The assessors also looked into whether and to what the extent the financial intelligence generated by the FIU is used in criminal investigations (particularly for ML) and prosecutions and possible convictions for ML.

Materiality

42. Like many European economies, Czech Republic's economic activity centres on services (62,3%). Industry stands at 35% of the economy; agriculture accounts for 2.8%. The main pillars of the Czech industry are engineering and machine engineering, mining, chemistry and food processing, followed by the energy industry, civil engineering and the consumer industry. In 2016, the gross domestic product (GDP) of the Czech Republic was USD 195.31 billion (EUR 157.94 billion). The GDP growth (4.6% increase compared to 2015) was driven by increasing household consumption. The new inflows from foreign direct investments amounted to USD 6,497 million (EUR 5,254 million) in 2016.

43. In global terms, the financial sector is medium to relatively small: the country is ranked in the Global Financial Centres Index 19 (GFCI 19) at 57th out of 86. The banking sector, which was comprised of 45 banks in 2016, is liquid and profitable. It consists of four large banks, which is the largest component of the sector sharing in total banking sector 59.3% of the assets. Out of the 45 banks, 23 are foreign bank branches (e.g. Polish bank PKO BP S.A., Czech Branch, established a branch on the domestic market in October 2016). Notwithstanding the number, foreign bank branches,' total banking sector assets declined from 7.9% in 2015 to 7.1% in 2016. Czech banks' return on assets and (especially) return on equity are generally higher than in other CEE economies, and are very high by Western European standards.

44. At the end of 2016, foreign owners controlled 93.1% of the assets of the Czech banking sectors (i.e. foreign bank subsidiaries or foreign bank branches), with 92.7% of the assets owned by foreign entities from EU Member States. In 2016, Czech banks directly managed CZK 5,960.9 billion (EUR 235.54 billion). Equity is the primary source of funding for the banks' business activities. As of 31 December 2016, accumulated equity amounted to CZK 540.8 billion (EUR 21.36 billion). Assets denominated in foreign currencies ("foreign currency assets") in the domestic banking sector amounted to CZK 1031.4 billion (EUR 40.74 billion) at the end of 2016. With a 56.1% share, foreign currency loans and other receivables are the largest item of the foreign currency assets of the sector as a whole. Other large items of foreign currency assets included deposits with other credit institutions with a 20% share and debt securities in banks' portfolios with a share of almost 17%.

45. A new fiscal responsibility framework was adopted in January 2017 by the Czech government. The law establishes, *inter alia*, an independent fiscal council to assess compliance with the fiscal rules and evaluate the long-term sustainability of the public finances.

Structural elements

46. The structural elements for effective AML/CFT controls are generally present in the Czech Republic. Although the country has experienced problems related to corruption and organised

crime since its transition to democracy in 1990, it is considered to be a consolidated democracy (it scored 2.25 out of 7 in Freedom House Nations in Transit 2017 ranking). The Czech Republic's electoral processes, local democratic governance and judicial framework and independence are well rated. However, less positive results were observed the national democratic governance processes, the level of corruption and the independence of media[5].

47. The Czech Republic has made a clear high-level commitment to implement the FATF standards, as well as the 4th AML Directive of the European Union, with a view to establishing an overall effective national AML/CFT framework. The NRA, as guide for a coherent risk-based approach, served as a trigger for important reforms to ensure a more effective allocation of financial and human resources, both in the public and private sectors.

Background and other contextual factors

48. The level of corruption represents a significant vulnerability in ML/FT risks. The NRA makes note of the study of the National Economic Council of the Government (NERC) which shows that corruption in relation to the state budget alone causes damage in the order of tens of billions of crowns (estimate for 2010 is CZK 39 billion/EUR 1,5 billion). Corruption risks in the public procurement sector are perceived to be especially high, but many other sectors, including public administration, carry moderate corruption risks. There is a moderate risk when dealing with the judiciary, particularly for bribes and irregular payments[6]. Moreover, in 2014, more than half of citizens perceived the police as corrupt[7]. Among the security forces corruption poses a problem; in 2015, the police investigated 174 cases of corruption among its own structures[8]. Another problematic factor for doing business and the efficient application of the AML/CFT framework is inefficient government bureaucracy[9]. Over two-thirds of businesses consider corruption to be widespread in national and local public procurements[10].

49. The most apparent evidence of corruption in the Czech Republic is indicated by the Panama Papers scandal of 2016. Among the countries mentioned, the Czech Republic appeared in more than a quarter-million documents and 283 Czech clients and shareholders were mentioned. Among them are people prosecuted and sentenced for financial crimes, lobbyists, diamond traders or people linked to the biggest privatisation and corruption scandals of the past two decades. The Czech bank eBanka, closed in 2008, was commonly used for money laundering.

50. One corruption case started in 2013 with a raid against organised crime, which involved several highly positioned state officials and politicians, as well as controversial entrepreneurs and lobbyists. The raid started after accusations and investigations into attempts to influence state institutions by lobbyists and state officials. It eventually led to a scandal in which Prime Minister Petr Nečas was affected, which resulted in the resignation of the Prime Minister and the cabinet. Moreover in 2013, five former executives of MUS Coal Company were found guilty of fraud, money laundering and other crimes during the company's privatisation process in 1999. The Swiss Court, where the defendants were charged with the crimes, also indicated that the Czech Republic could seek hundreds of millions in funds seized by Swiss authorities from bank accounts linked to the privatisation of the coal mines. A recent case of high-level officials' corruption began in January 2018, when Andrej Babiš, Prime Minister and his cabinet were not

[5] https://freedomhouse.org/report/nations-transit/2017/czech-republic
[6] Global Competitiveness Report 2015-2016, World Economic Forum
[7] Special Eurobarometer 397, European Commission, February 2014
[8] Czech Republic 2016 Human Rights report, U.S Department of State
[9] Global Competitiveness Report 2015-2016, World Economic Forum
[10] Special Eurobarometer 397, European Commission, February 2014

given the vote of confidence by the Parliament, over allegations that he had abused an EU subsidy programme in 2007.

51. The government has developed several anti-corruption measures, such as the Government Concept of Combating Corruption, the Action Plan to Combat Corruption and basic principles of combating corruption. However, according to Transparency International, the anti-corruption legislation is still inadequate. This becomes clear in the law on lobbying, the law on whistle blowing and the law on the powers of the supreme audit office, which are the laws that were not passed by the parliament. Some laws, e.g. on party financing or on conflict of interest and other regulations, were adopted but different views were raised with regard to their qualities[11].

52. The NRA indicates that the Czech Republic is aware of the risks and that the country pays considerable attention to corruption issues in its strategic documents. The following legal reforms are either underway or have been recently completed: 'Financing of political parties and election campaigns' (amendment of Act No. 424/1991 Coll., on association in political parties and political movements and amendments to electoral laws); Proposal of Act on Proof of Origin of Assets (to modify existing tax law mechanisms so that it is possible to detect unreturned or concealed incomes of taxpayers and tax them); amendment to the Criminal Code implementing the so-called confiscation directive (the Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the confiscation of instrumentalities and the proceeds from crime in the European Union); Proposal of Act on Public Prosecutor's Office (Parliamentary Press NO. 789); Act on the Register of Contracts (340/2015 Coll., entered into force on 1 July 2016); Amendment to the Act on Conflict of Interests (amendment to Act no. 159/2006 Coll. On Conflicts of Interests, as amended); Act on Public Procurement (Act no. 134/2016 Coll., On Public Procurement, came into effect on 1 October 2016); Amendment to the AML Act (i.e. transposing the 4th AML Directive, effective from 1 January 2017); the CZ10 Project: Project to strengthen the fight against corruption and money laundering in the Czech Republic (Norway Grants: 2009-2014).

Overview of AML/CFT Strategy

53. The NRA aims to formulate a national AML/CFT strategy, as well as to contribute to the national AML/CFT policy. In line with this policy, the Czech Republic introduced a number of measures in recent years to strengthen its fight against economic crime.

54. From an institutional point of view, the Financial Analytical Unit (acting as an FIU) is considered as the main actor in the AML/CFT policy making.

55. The results of the NRA indicated a set of measures to be taken to improve the national AML/CFT framework. A timeline is also provided for a coordinated approach to improve the AML/CFT policies. A date of implementation, the implementer and the measure to be taken, is given for every risk identified in the NRA.

Overview of the legal framework

56. ML is criminalised mainly under Sections 216 and 217 of the CC, as well as under several Acts and Regulations, such as Act No. 253/2008 Coll. On 'Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism' (last amendments: Act no. 368/2016 Coll., effective since 1 January 2017 and Act No. 183/2017 Coll., effective since 1 July

[11] *Why the Czech Republic scored worse in corruption index*, 01 February 2017, Radio Praha. http://www.radio.cz/en/section/marketplace/why-the-czech-republic-scored-worse-in-corruption-index

2017); Act No. 69/2006 Coll., on the "Implementation of International Sanctions"; Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 'Controls of cash entering or leaving the Community'; Regulation (EC) No 1781/2006 of the European Parliament and of the Council on 'Information on the payer accompanying transfers of funds'; and Decree No. 281/2008 Coll., of 15 August 2008, as amended, on 'Selected requirements regarding the system of internal principles, procedures and control measures against legitimisation of proceeds of crime and financing of terrorism'.

57. At the time of the adoption of the 4th round MER on the Czech Republic (April 2011), criminalisation diverged from the standards provided by the Vienna and Palermo Conventions. It was found that the coverage of money laundering in the Czech CC was not sound and consistent. The evaluators indicated that the inconsistencies regarding the definition of the offence went against a coherent treatment of the criminal phenomenon of ML; the fragmented approach might lead to the dilution of the ML concept and, hence, the respective offences; and the court practice had illustrated that the legalisation offence had mostly been applied to criminal offences which had more to do with stolen goods than with the classical laundering of profits obtained through criminal activity.

Overview of the institutional framework

58. The institutional framework for the development and implementation of the Czech Republic's AML/CFT policies includes the following agencies:

59. The **Financial Analytical Unit (FAU)** is the coordinator of the NRA process, and also functions as the umbrella for the system of AML/CFT prevention in the Czech Republic. It receives, investigates, processes and analyses STRs; it files criminal complaints; and provides information to the relevant bodies active in the fight against ML/FT. The FAU is also authorised to control FIs and non-FIs and their compliance with the AML/CFT obligations. It can impose sanctions in case of breach of these obligations. The FAU acts as the FIU of the Czech Republic in international co-operation and is the competent authority in implementation of international sanctions. In connection with international sanctions, the FAU is allowed to receive information about the location of assets which are subject to the international sanctioning regime, handle and manage these assets and administer them after delivery or dispossession; and to grant an exception from the sanctioning regime and impose administrative sanctions for a breach of obligations as stipulated under the Czech Sanctions Act. Lastly, the FAU is responsible for the application of the following pieces of legislation: AML Act, Sanction Act and Act No. 300/2016 Coll., on the central Registry of Bank Accounts, and implementation of EU legislation in the field of AML/CFT.

60. The **Police and National Organised Crime Agency of the Police (NOCA)**, acting as a law enforcement authority, has the main responsibility for the investigation into ML/FT and associated predicate offences. It investigates in the areas of, e.g. organised crime; economic crime and corruption; terrorism and extremism; cybercrime; and financial crime; and crimes executed by or under the auspices of high-level authorities. It acts as a main law enforcement agency in financial investigations.

61. The **Ministry of Justice** creates the conditions for the courts' and prosecutors' offices' due performance of tasks resulting from the Constitution and from other laws. It fosters the required conditions for the failure-free operation of the courts, prosecutors' offices and other bodies; it stipulates forms and methods of managerial and supervisory activities of chairs of the courts and lead public prosecutors during the exercise of their administrative functions and audits the observance of these forms and methods; it ensures professional training and further

education of judges, public prosecutors and other personnel; and cooperates with the Czech Union of Judges, the Union of Public Prosecutors and other professional organisations and trade unions. The Ministry of Justice is also involved in the area of MLA occurring during court proceedings in ML/FT cases. It has no right to issue any binding instruction, but instead provides guidance documents to assist judges in their participation in international legal cooperation. Lastly, the Ministry is responsible for coordination of different legislative initiatives in criminal and civil law matters, which also include respective AML/CFT components.

62. The **Ministry of Finance** is responsible for creating the legislation related to the capital market, payment services, insurance sector, employees' pension insurance and retail financial services. It also ensures the implementation of the EU legislation. Together with the Customs Administration and the FAU, the Ministry of Finance acts as supervisor of the gambling sector. It oversees the online operators and has no authority in the light of AML.

63. The **Czech National Bank (CNB)** is an AML/CFT supervisor of all financial institutions. It is also responsible for licensing of financial institutions. The CNB has the power to conduct corresponding enforcement proceedings should it identify any breaches of AML/CFT obligations. It is one of the key counterparts to the FAU in the field of AML/CFT policy making, legislative reform and awareness-raising activities.

64. The **Public Prosecutor's Office** comprises a system of state offices designated to represent the state in matters of protection of public interest in cases entrusted to it by the law. It represents public action in criminal proceedings and performs additional tasks stipulated by the law. Their responsibility includes detection, prevention and suppression of ML/FT within the scope of criminal proceedings. In pre-trial proceedings, the public prosecutor is the dominant body. It is obliged to prosecute all criminal offences of which they gain knowledge, unless the law or a promulgated international treaty binding the Czech Republic stipulates otherwise.

65. The **Customs Administration** is responsible for overseeing the land-based operators and shares the authority in the sense of the AML with the FAU. It controls the compliance with the obligations to identify the customers and performs a CDD. It also conducts the administrative proceedings in case of detection of any offence. Moreover, the Customs Administration is responsible for detection, monitoring and reporting of cash transactions. It controls the fulfilment of the obligation to file a cash transaction through announcement forms, and it provides these forms to the FAU.

66. The **Czech Bar Association** has a primary role to ensure that the system covers the widest possible range of bodies and organisations that contribute to the performance of the set of tasks in public interest. It plays a balancing role between two public interests (lawyer's professional secrecy and the prevention of all practices associated with ML/FT), and it performs supervisory activities, trainings and education.

67. The **Notarial Chamber of the Czech Republic** acts as an intermediary between the notary and the concerned authorities.

68. The **Bailiff Chamber of the Czech Republic** associates all judicial officers, and supervises over the activity of the judicial officer, which includes the observance of duties imposed upon the judicial office by the AML/CFT Act.

Financial Sector

69. The majority of entities providing services on the financial market are supervised and licensed by the CNB. The CNB supervisory role is shared by two of its departments: The Financial Market Supervision Department I (banks including foreign bank branches; credit unions; life insurance companies; and pension companies) and The Financial Market Supervision Department II (capital market sector; Non-banking credit providers sector; and Currency exchange offices sector and non-banking payment service providers sector).

70. There are 58 banks and cooperative savings in the Czech Republic and majority of banks are part of the European banking groups. The banking sector consists of four large banks (which hold 60% of total banking sector assets), five medium-sized banks and nine small banks, along with five building societies and 24 foreign bank branches. The banking sector is dominated by foreign banks. 93% of the assets of the Czech banking sector are under the direct or indirect control of foreign owners.

71. The insurance sector is represented by life insurance companies and insurance intermediaries. According to the information from supervisors there are 20 life insurance companies, 3 of which are foreign insurance branches from EU, and 154 355 insurance intermediaries. Since 2012 this number increased with approximately 20.000 entities.

Table 1: financial sector in the Czech Republic

Financial Institutions		
Sector	**No. of Registered Institutions**	**Value of assets (EURO[12])**
Banks and cooperative savings	58	265,6 bn
Life insurance companies	20	18,02 bn[13]
Insurance intermediaries	154 355	N/A
Non-bank payment service providers or electronic money issuers	209	2,6 bn
Agents of Foreign payment institutions from MS		
Securities – investment firms	66	1 bn
Investment companies	27	14,79 bn
Self-governing investment funds	29	2,08 bn
Non-bank foreign exchange entities	1 004	N/A
Pawnshops		
Lenders and credit intermediaries other than banks and savings banks		
Pension companies	8	17,0 bn

[12] Exchange rate as of June 30, 2017
[13] According the Czech Generally Accepted Accounting Principles

DNFBPs

72. The DNFBP sector in Czech Republic consists of casinos, real estate agents, lawyers, notaries, tax advisors[14], bailiffs, accountants, auditors, dealers in precious stones and metals, trust and company service providers.

73. Only licensed casinos can operate in Czech Republic. There 262 land-based and 1 internet casinos according to the information as of 30.06.2017. All casinos are supervised both by Ministry of Finance and municipal authority.

74. There is no available information on number of licensed real estate agents. Currently the Ministry of Regional Development proposed changes in legislation to enhance the process of authorization of real estate agents.

75. Lawyers and notaries are supervised and licenced by their professional chambers (the Czech Bar Association and the Notarial Chamber of the Czech Republic). There are about 12 900 licenced lawyers and 449 notaries in Czech Republic. Both chambers control professional qualification and absence of criminal records of their members.

Trusts are a fairly new concept in the Czech Republic and they are not very material as they represent less than 1% of the most used forms of legal persons. The Czech Civil Code distinguishes the usual three basic entities - the founder, the beneficiary and the trustee. In the Czech Republic the purpose of the trust may be either publicly beneficial or private.

76. All obligated entities, including accountants, are supervised by the FAU with the exception of other legal and advisory professions which are supervised by their chambers. No specific certification is required for the other DNFBPs, except accountants where professional license is voluntary.

DNFBPs in the Czech Republic

Casinos	263
Real estate agents	N/A
Lawyers	12.901
Notaries	449
Tax Advisors	4.703
Bailiffs	154
Accountants	N/A
Auditors	1.598
Dealers in Precious Metals and Stones	N/A
Trust and Company Service Providers	406

Overview of preventive measures

77. The applied measures are generally consistent with the risks identified through the NRA. However, these measures are not always proportionate to the level of acknowledged risks or vulnerabilities. The knowledge of the DNFBPs on AML/CFT preventive requirements is uneven: some DNFBPs act preventively in their application of the measures while others are less developed. This indicates an unequal level of understanding of AML/CFT preventive requirements.

[14] In Czech Republic tax advisors are considered as 'other legal professionals' in line with Art 2(3) latter a) of the IV EU AML Directive.

78. FIs demonstrate an adequate application of the CDD regime. The reporting entities cannot establish business relationship with clients if they refuse identification. The verification of the BOs is done using public sources and data from the Commercial Register after the examination of the "solemn declaration" given by the client.

79. An increase in the quality of STRs, especially when received from banks has been noted. However, compliance with the reporting obligations by DNFBPs is an area for improvement. The same imbalance is noted with respect to application of AML/CFT internal control procedures requirements.

Legal persons and arrangements

80. There are three essential types of legal persons that can be established according to the Czech Civil Code - corporations, endowed institutions and institutes. The Civil Code regulates two types of corporations: association (Section 214) and association of unit owners (Section 1194); two types of endowed institutions: foundations (Section 306) and endowment funds (section 394) and institutes (Section 402). According to the Business Corporations Act corporations can be divided into commercial companies and cooperatives. It also provides more detailed regulation of legal persons: unlimited partnerships (Section 95), partnerships (Section 118), limited liability companies (Section 132), joint-stock companies (Section 243) and cooperatives (Section 552).

Table 2

Type of Legal Persons / Arrangements	No. Registered (where available)
Limited liability company	442110
Joint-stock companies	26368
Limited partnership	738
Unlimited partnership	6399
Cooperative	14425
European Company	2014
European Cooperative Society	1
European Economic Interest Association	10
Trust	406
Association	96578
Foundation	569
Endowment fund	1851
Institute	830
Publicly Beneficial Association	2931
Professional Association of Legal Persons	1323
Labor Union	1190
Employers Organization	
Political Party and Political Movement	238
Church	38
Religious Organisations	5308
Hunting Association	4227

81. All legal persons are required to be registered in a public register. There are several public registers of legal persons in the Czech Republic which can be accessed directly through the internet and the Register on Beneficial Owners which was established in 2018. The access to

the Register on BO is available only to the relevant authorities, as prescribed by the law. All legal persons have to be registered both in a public register and the Register on BO.

82. All information on trusts has to be registered in the Register of Trusts and competent authorities and obliged entities have access to it. The information includes the beneficial owner, the residence of trustee, and the purpose of the trust. There is no requirement for trustees in the AML/CFT Law to disclose their status to obliged entities, but they are obliged present documents for tax purposes including data on bank accounts.

83. The non-profit sector in Czech Republic includes associations, public benefit companies, institutes, religious legal persons, foundations and endowment. Information on NPOs is kept in public registers except information on beneficial owners which is accessible for LEAs. According to the legislation all NPOs are obliged NPOs to provide annual reports and financial statements to the Register Court. The NRA noted the fact that the risk of abuse of NPOs to support and fund terrorism has been considered by the authorities, but yet not fully determined.

84. There is no full assessment of the vulnerabilities of legal persons that can be created in the country. However, there are no suspicions for abuse of legal entities for FT purposes.

Overview of supervisory arrangements

85. Licensing, regulation and supervision of financial institutions and DNFBPs is undertaken by a number of different authorities.

Name of the sector/services	Licensing requirements	AML/CFT Supervisor
FIs		
Banks	Licensing	CNB and FAU
Lending, leasing and factoring	Licensing	FAU and CNB
Payment institutions	Licensing	CNB and FAU
Money and value transfer services (including by Post office)	Licensing	FAU
Foreign currency exchange offices	Licensing	CNB and FAU
E-money institutions	Licensing	FAU and CNB
Savings and loans associations and their unions	Licensing	FAU and CNB
Insurance companies	Licensing	CNB and FAU
Collective investment bodies (investment funds and management companies)	Licensing	CNB and FAU
Securities brokerage companies	Licensing	FAU and CNB
Investment advisory company in securities	Licensing	CNB and FAU
Custodian services	Licensing	FAU and CNB
Voluntary pension funds and management companies	Licensing	CNB and FAU
DNFBPs		
Gambling providers	Licenced	FAU & State Supervision of Betting Games and Lotteries
Notaries	Licensed	The Notarial Chamber
Lawyers	Licensed	The Czech Bar Association
Auditors & accountants	Licensed (voluntary)	FAU
Real estate agents	No specific certification	FAU
Trade in precious metals and precious stones	No specific certification	FAU

International cooperation

86. The FAU has power to exchange information (whether classified or not) on ML and FT, with foreign counterparts, including non-FIU authorities, both spontaneously and upon request. Cooperation is provided on the basis of the principle of reciprocity or MOUs. MLA requests are executed within 20 days for a regular request, and 5 days in case of urgent request. Exchange of information is secured and conducted via secure gateways (ESW and FIU.Net). Measures to protect information from unapproved dissemination are in place.

87. The legal basis for LEAs international cooperation is in place. The LEAs exchange information with their foreign counterparts with Interpol, Europol, CARIN, ARO, EPAC, StAR, relevant authorities and institutions of the European Union and its Member States, as well as with other international organisations, foreign security forces and other competent foreign entities both spontaneously in the context of its EU membership and within joint investigation teams. Coordination of MLA can be provided also by Eurojust, CARIN, EJN and other specialised networks. Prioritisation of requests and the required execution processes are in place and regulated by several internal instructions.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

- The NRA was a nation-wide exercise conducted over the years 2015-2016. The report appears to be the result of a transparent and realistic analysis of the ML/FT risks faced by the country. Whereas the assessment took on the majority of key risk areas fairly thoroughly, certain aspects of risks identified in the NRA, such as laundering of foreign proceeds, the use of instruments of fictitious entrepreneurships, real estate business or risk posed by organised crime require further analysis and subsequent mitigation measures.

- The private sector contributed, to a certain extent, in identifying key ML/FT risk. The FAU provided sector-specific versions of the NRA to the reporting entities, and prepared the general structure of the risk assessment which should be used by the private sector when performing their own evaluation of risks. The FIs undertook an internal risk assessment exercise, using the NRA, group-wide risk evaluations and external sources.

- Significant effort has been devoted by the FAU to raise awareness on the findings of the NRA. Whilst the understanding of risk level by those entrusted with the NRA exercise appears to be high, the specific levels and prioritisation of different categories of risks could have been expressed in a clearer and more user friendly manner. In other words, the conclusions should have led the reader to easily establish the priorities as between different risk areas.

- The various authorities to whom the NRA is addressed demonstrated different levels of understanding of their own risks against the backdrop of the NRA. These discrepancies are even more present with respect to private sector entities. Whilst the financial institution (e.g. banks) demonstrated a relatively high level of understanding and awareness of ML/FT risks, the same cannot necessarily be stated for certain other reporting entities.

- In parallel, and for the general public, the Ministry of Interior developed the National Security Audit, which examines, inter alia, the threats related to terrorism, terrorism financing and organised crime. Since the NSA looks at several relevant areas, it remains unclear why the analysis therein was not fully integrated with the NRA.

- The Action Plan resulting from the NRA did not focus sufficiently on future actions, since in many cases it suggested measures that had already been either initiated or entirely carried out. Whilst the Government is responsible for overseeing the implementation of the Action Plan, no report on the status of this matter is currently available.

Recommended Actions

- Update the NRA so that it clearly indicates the ML and FT risk levels associated to different risk areas. Update the Chapter 4.1 of the NRA, revise the measures included therein, focus more on the actions which resulted from the analysis of risks and specify their intended outcomes in order to allow for proper monitoring of their implementation.

- Undertake a more detailed assessment of FT risks, use the NSA findings on threats in this endeavour and cover all FT related risks which were overlooked in the NRA.

- Strengthen the use and provide clear terms of reference of the existing coordination platforms which are responsible for the NRA's updates and follow up. This should include a

designation of the monitoring body tasked with oversight and reporting on implementation of the mitigating measures foreseen in the Chapter 4.1.

- Improve the understanding of risks by certain private sector entities (capital market participants and the currency exchange bureau, real estate, DNFBPs) and engage them more closely in targeted analysis of specific sectors risks.

- Review AML/CFT Law and introduce (i) an obligation to conduct EDD where the ML/FT risks are higher and (ii) revise the requirements for simplified CDD in order to correctly reflect the results of the NRA, and of the risk assessments carried-out by each obliged entity.

Immediate Outcome 1 (Risk, Policy and Coordination)

Country's understanding of its ML/TF risks

88. The NRA was approved by the Government of Czech Republic on 9 January 2017 (Resolution no.5/2017). The document addresses both ML and FT risks and includes assessment of threats, vulnerabilities and consequences. The NRA states that '*the information contained herewith are intended for third parties, can only be used for the purpose of ML/FT prevention and is a subject to confidentiality pursuant to the AML Act, as amended*.' It also sets specific mitigating measures to address the risks identified. As a matter of fact, these mitigating measures are an integral part of the NRA report.

89. The overall NRA process was steered by the FATF Guidance on National ML/FT Risks Assessment - the authorities applied in-house methodology which was informed by the core principles and contexts elaborated in this FATF document. The process was coordinated by the FAU and involved relevant authorities such as Police, Public Prosecutors, different sectors supervisors (Czech National Bank, Czech Trade Inspection, gambling supervisory), self-regulatory bodies (e.g. legal professionals Chambers), regulators and policy makers (Ministries of Finance, Justice, Interior, Culture), Tax and Customs Administrations, specialised Government Council on NPOs, Anticorruption Committee and the private sector – the last being mostly represented though different obliged entities (e.g. credit institutions, security market intermediaries, payment services providers, insurance industry, bureaux-de-change, gambling operators, legal and advisory professions and trust and company services providers) and mostly during the NRA report drafting stage. Some specific consultations with entities not directly concerned by the AML/CFT legislation (e.g. the Ministry of Regional Development) were also held. The NRA was published on the FAU website[15] and thus made available to all interested parties and public in general.

90. Government approval of the NRA also triggered additional action by the FAU – twelve non-public tailor made analyses of risks which correspond to specific segments of the private sector (i.e. groups of obliged entities with roughly similar types of products and services and their exposure to ML/FT risks) were produced and delivered. These analyses are confidential and they were distributed to the relevant reporting entities, although the entities which have not received their respective analysis are given an opportunity to contact FAU to obtain the analysis tailored to them. The authorities advised that these so called 'single sub-processes' included in-depth discussions with relevant stakeholders (including the private sector) and their comments and suggestions were given due consideration.

[15] http://www.financnianalytickyurad.cz/download/FileUploadComponent-1830718990/1489152816_cs_zpravaverejna.pdf

91. The NRA is reasonably comprehensive, given that it was the first wholesale process of identifying ML/FT risks in the country. It has clearly aided the understanding and knowledge of the competent authorities and the private sector in relation to the threats and vulnerabilities they face. The analysis of threats includes primarily typologies accompanied by information on types of obliged entities exposed to such *modus operandi*. In addition, the typologies were complemented by: i) the risk factors (related to a customer, a service or a transaction) such as: the scope of business or type of commodities (usually those that might be at risk when it concerns ML), vulnerable legal entities or arrangements; and ii) the most common indicators which obliged entities use to detect suspicious transactions. Nonetheless, the classification of risks as per their importance appears not to be comprehensive enough. The heat map provided at the end of the NRA (Chapter 4.1) does include the ratings associated to different risks, but the assessment team is of the opinion that the reporting entities and other interested interlocutors would further benefit from a more reader-friendly statement of the specific risks ratings. In addition, such a presentation could have also been included in the introductory/executive summary part of the document.

92. The NRA also identified and assessed the vulnerabilities arising from PESTEL[16] analysis (Chapter 3.3), the scope of which included three areas: 1) Corruption as a Vulnerability Relevant for ML/FT Risks; 2) Vulnerability of Non-Profit Organisations in terms of ML/FT, and 3) Vulnerabilities in the Prosecution of Crime. The analysis includes current threats identified in these areas, measures in place and possible new measures that will be fully formulated once the results of those already in place are further assessed.

93. The threats were considered in light of three different components: i) their seriousness; ii) probability/frequency of their occurrence, and iii) their 'dangerousness' (i.e. damage they can cause to the public interest; whether they could be done in an organised manner; difficulty to detect them, etc.). Consequently, tax crimes, fraud, corruption, phishing, and subvention frauds (otherwise known as "Subsidies Fraud", i.e. the abuse of government subsidies programs) are found to be the most common predicate offences which trigger subsequent laundering of proceeds. FT, for example, was also under scrutiny due to its seriousness, whilst, on the other hand, it was concluded that the probability of its occurrence was low.

94. The extent to which legal entities are abused for ML/FT purposes has been analysed only within the typologies presented. In other words, the NRA does not provide a specific list of risks in relation to how legal persons can be used for laundering purposes. For example, the risks and vulnerabilities related to the possible usage of fictitious entrepreneurships for ML have not been thoroughly explored. This appears to be a significant threat due to the fact that creating or purchasing an already existing company (including shell companies) is a very simple procedure. This might, in practice, attract criminals or organised criminal groups to set up or purchase companies and use fictitious devices (such as straw men). The risk of fictitious entrepreneurships was confirmed by the LEAs, but the NRA discussed only a potential threat of shell companies, and BO related risks as a part of typologies observed. Whilst the overall understanding of these risks among relevant authorities appears to be satisfactory, the assessment team is of the opinion that a more thorough analysis of these threats should have been included in the NRA.

95. The understanding of risks is somewhat impaired in relation to how, and to what extent, Czech authorities have considered the financial flows from abroad and their impact on ML/FT threats and vulnerabilities. In particular, the internationalism of the banking sector, although not

[16] An acronym based on the first letters of the major categories: political, economic, social, technological, environmental and legislative

being significant, could reveal certain typologies especially as concerns money flows from the Far East and former Soviet Union. Although some typologies which include this element are offered in the NRA, the analysis appears to lack the assessment of data with regard to the geographic origin of customers and beneficial owners. Nonetheless, the threat of laundering of foreign proceeds, in terms of its severity, is considered low; in terms of its frequency is considered moderate; and in terms of the degree of consequences (dangerousness, damage to public interest, organisation, difficulties in detection, etc.) is considered low as well.

96. Similarly to financial flows from foreign jurisdiction, certain important sectors warrant a more prominence in the overall analysis. This primarily concerns risks of laundering of proceeds through real estate. During the on-site visit, the authorities stated that the scope of the sector, level of its exposure to ML risks, and cases examined so far, did not warrant the same level of analysis as some other sectors. Nevertheless, the Chapter 4.1 lists the ML threats presented by the real estate sector as high, whilst the same applies to the real estate agencies' exposure to ML related threats and vulnerabilities. The way real estate can be purchased in Czech Republic (e.g. no notary's deed is needed, simple transfer of money and a signed contract between the parties is sufficient to register as an owner) is certainly an argument in favour of further analysis of the sector. In addition, there are no requirements in place for real estate agents to be registered or licensed, nor do they need to be a member of their association. This issue was not addressed in the NRA thus no mitigating measure was foreseen in the action plan. The assessment team view is that these factors significantly increase the risk of integration of foreign criminal assets into real estate sector.

97. In 2016, in parallel with NRA, the Ministry of Interior developed the National Security Audit (NSA)[17] with the idea of presenting the wider public the capacities of the Czech Republic to deal with the emerging problems that resulted from the migration crisis. This was a nation-wide project and involved academics, LEA professionals, NGOs, etc. and included numerous discussions and debates on different security risks. The NSA Action Plan was developed by LEAs and remained confidential. Furthermore, the NSA assesses, inter alia, terrorism, FT and organised crime related threats and vulnerabilities. Although the NSA is not officially a part of the NRA, the authorities advised that the NSA informed the NRA.

98. The NSA also assesses as "high" the threat of: penetration of organised crime into public administration and law enforcement authorities; abuse of public procurement and public budgets; tax evasion, etc. A "medium" level of threat is associated to FT and other activities to support terrorism; abuse of conventional weapons and weapons of mass destruction, explosives and dual-use technologies; foreign terrorist fighters and terrorists acting alone. The NSA also highlighted a number of weaknesses, which included, insufficient staffing and an inadequate legal framework (in the cybercrime field); lack of expertise in detecting and investigating tax and serious economic crimes; and problems in international cooperation with geographically and culturally distant countries.

99. The risk of FT has been the subject of attention and scrutiny by the authorities. The interviews held onsite confirmed that LEAs made efforts to identify the sources of funds that can potentially be used for the purpose of FT, such as activities related to potential recruitment, radicalisation and self-radicalisation of individuals. However, the risks concerning foreign terrorist fighters could perhaps have been elaborated more thoroughly. As it happens, an incident of this nature occurred (though this attempt to join ISIL was successfully thwarted by the Czech authorities) shortly after the NRA was approved.

[17] http://www.mvcr.cz/cthh/soubor/national-security-audit.aspx

100. The risk of terrorist abuse in the NPO sector and the problem of cash smuggling in the FT context, were also considered in the NRA.

101. One positive impact of the NRA has already been evident in the LEAs' efforts to respond to the threats and vulnerabilities in investigating and prosecuting ML/FT and proceeds generating crimes. The actions triggered as a result of the NRA analysis predominantly involve capacity building of the NOCA and prosecution services – as an example, both institutions strengthened their capacities to combat tax evasion, serious frauds and anti- terrorism, updated their strategy on combating organised crime and strengthened cooperation with the Tax Administration.

National policies to address identified ML/TF risks

102. Several strategic documents, such as the National Strategy for Combating Terrorism (2013) and related Action Plan (for the period 2016 – 2018), the Strategy for Combating Organised Crime (for the period 2015 – 2017), have been in place and served the authorities in identifying immediate and long term objectives in these areas. The NRA also notes that *on the national level and with respect to prevention and mitigation of ML/FT risks, the aim is to formulate a national AML/CFT strategy.* At the time of the onsite visit, a unified national AML/CFT strategy, which would combine the results of the National Strategy for Combating Terrorism, the Strategy for Combating Organised Crime, the National Security Audit and the National Risk Assessment had not yet been developed.

103. As for direct measures to mitigate ML/FT risks, the Czech authorities considered it best to include them in the NRA document. In other words, the Action Plan provided in the Chapter 4.1 of the NRA, includes: i) a description of the risk; ii) its source of identification; iii) a reference to the chapter of the NRA which elaborated on the risk; iv) an assessment of its seriousness; v) a description of the mitigating measure(s) foreseen; vi) type of measure (e.g. whether it is legislative or institutional reform); vii) the institution(s) in charge for implementing it; viii) a deadline for its implementation; and ix) the nature of the measure in terms of the overall AML/CFT system (e.g. whether it is a preventive, analytical or investigative measure). The assessment team, following the meetings held on-site, was assured that strong and demonstrable political support for proper and timely implementation of these measures is in place. This was also confirmed by the fact that numerous measures were already well advanced or even fully applied in practice (e.g. strengthening of the supervisory regime by FAU and CNB, introduction of the RBA; strengthening of the institutional capacities to respond to threats posed by specific crimes and confiscate the proceeds thereof, etc.).

104. However, it appears that the Action Plan (AP) focuses mostly on the measures that have already been implemented (e.g. through various legislative amendments) or whose implementation is underway, whilst future actions have rarely been introduced. In addition, the diversity/type of the actions and their implementation could have been better defined. For instance, some measures are quite broad (e.g. the risk is described in Chapter 3.1.5 of the NRA as '*Cash payment transactions, risk of involvement of agents/sales representatives (money remittance) cash-less transfers'* with the mitigating measure of '*setting up of a management and controlling system.*' This type of measure is defined as '*CDD, transaction, monitoring, systematic control of agents/sales representative*'.) For this particular measure the implementation date is noted as '*continuously (already in the current legislation)*', the implementing agencies being the obliged entities with payment services. This example suggests that some of the measures repeat certain requirements embedded in the legislation rather than raising an issue which would be a new deliverable of the analysis of risks in the area. In addition, it is merely the law which requires monitoring of implementation of this measure, putting in doubt any added value of having this particular action in the AP. This is the case with some other measures.

105. The format of the AP is somewhat ambiguous – the risks and the mitigating measures were not classified by specific criteria but rather appear to be randomly dispersed throughout the AP and distinguished only by the colour-coded risk levels attributed to them on a graphic table. The assessment team is of the opinion that the clear distinctions among different parts of the AP could have been based on certain criteria such as the nature of the action (e.g. preventive or repressive), agencies in charge of their implementation (e.g. FAU, LEAs or these requiring a multi-agency approach), implementation deadline, etc. In addition, perhaps each risk and its mitigating measure(s), for ease of reference, could have been given an action plan reference number. Such format would then be more reader-friendly and would enable authorities to better oversee and monitor its implementation.

106. As already noted, the NSA also proposes certain measures of relevance for AML/CFT, terrorism and confiscation of proceeds of crime. Whilst this action plan is confidential, authorities advised that no discrepancy exists between this action plan and the one based on the NRA. Authorities also advised that the NSA action plan largely served professionals to further develop their work, as it mostly concerned the transportation of cash, money mules, inadmissibility of intelligence in criminal procedure, converting intelligence into evidence, etc. Nonetheless, information is not available on the number of measures implemented or the overall percentage of measures of this action plan completed so far.

107. Despite the shortcomings noted above, meetings held on-site demonstrated to the assessment team the overall commitment by the authorities to apply the mitigating measures. Almost all interlocutors were aware of the measures assigned to them and confirmed their readiness to respond to their requirements.

Exemptions, enhanced and simplified measures

108. The lower risk scenarios for the application of simplified CDD measures are provided in Art. 13 of the AML/CFT Law in relation to certain institutions and services (i.e. credit or financial institutions; securities companies operating on the regulated market, local government authorities, insurance policies with low premiums etc.). The inherent risks corresponding to these exemptions do not stem from the NRA or other risk assessment and are mostly based on the examples provided in the Interpretive Note to FATF Recommendation 10. According to the authorities, the legal requirements for simplified CDD measures should be revised in order to correctly reflect the results of the NRA, and of the risk assessments carried-out by each obliged entity. The issue was included in Chapter 4 of the NRA "Summary of Risks and Necessary Additional Measures", and the FAU was designated as the responsible authority to propose the necessary amendments to the AML Act. No specific deadline to complete this action has been set.

109. Article 13A of the AML/CFT Law provides exemptions from identification and CDD, in relation to e-money and mobile payment services within value limits (the highest stored amount does not exceed EUR 250 or EUR 500 in case of electronic money). Unlike the simplified CDD, the exemptions do result from the analysis described in Chapter 3.1.5 of the NRA, which revealed no or very limited ML/FT exposure for the e-money and mobile payment services.

110. With regard to enhanced measures, the AML/CFT Act does not explicitly require obliged entities to perform ECDD where the ML/FT risks are higher. Thus, the NRA results do not directly support the application of enhanced measures for higher risk scenarios as this is not prescribed by the AML Law. The authorities argue that in practice the ECDD is applied, as the obliged entities are required to perform on-going monitoring of the business relationship taking into account the potential risk of legitimisation of proceeds of crime (i.e. ML) and financing or terrorism (see R10.17). The on-site meetings with the banks demonstrated that AML/CFT risk

mitigation measures are taken based on clients' risk profile, including the application of ECDD in cases of "negative" information acquired from paid databases (e.g. WorldCheck) or from public sources. However, this is not the case for all reporting entities, and legally there is no obligation to apply ECDD for risks identified, assessed and understood by the country (NRA).

Objectives and activities of competent authorities

111. The two main regulators engaged in the AML/CFT supervision in the Czech Republic are the FAU and CNB. They simultaneously and in parallel oversee the largest part of the financial sector and DNFBPs, and perform AML/CFT supervision. Other supervisors are the SRBs such as the Notarial Chamber or the Czech Bar Association and the Custom Administration. The AML/CFT degree of risk-based supervision varies significantly.

112. Following the NRA findings, the CNB decided to assign the supervisory activity to two of its departments, segregated according to the categories of supervised entities:

a) The Financial Market Supervision Department I responsible for the supervision of: banks including foreign bank branches; credit unions; life insurance companies; and pension companies;
b) The Financial Market Supervision Department II responsible for: the Capital market sector; the Non-banking credit providers sector; and the Currency exchange offices sector and non-banking payment service providers sector.

113. The Financial Market Supervision Department I applies a comprehensive risk-based supervision system, and has a team dedicated solely to AML/CFT matters, in order to ensure quality supervision by experienced and dedicated staff. The authorities informed the assessment team that the decision to establish a separate AML/CFT unit was taken based on the NRA findings which identified a higher exposure to the ML/FT risk by credit institutions. The Financial Market Supervision Department II includes AML/CFT issues in its general supervisory activities but would benefit from being more AML/CFT driven.

114. Given the findings of the previous evaluation and considerations about the low level of risk understanding by the DNFBPs, the assessment team paid particular attention to this segment during the on-site visit. The interviews held confirmed that the level of understanding of AML/CFT risks by DNFBP supervisors has improved since the previous evaluation. Based on the results of interviews conducted with professional chambers (lawyers, notaries, auditors, bailiffs and tax advisors) the awareness and understanding of ML/FT risks were moving towards a satisfactory level. The evaluation team was assured that, in the course of regular inspections performed by the professional chambers, AML/CFT aspects are also considered and some sanctions were in fact imposed for AML/CFT violations[18].

115. Whilst the NRA was completed with the participation of all relevant public institutions (and to a certain extent with contributions from the private sector), there is no authority routinely collecting and aggregating information across all sectors on, *e.g.* customer risk classifications, numbers and/or types of PEPs, residence of beneficial owners of customers, or the manner in which exemptions or simplified CDD measures are applied. The NRA does consider and assess the ML/FT risk of each financial sector, but there is no authority responsible for identifying and maintaining a global understanding of the ML/FT risk between different sectors and type of institution, or allocating resources based on such an understanding. The focus is placed on risk assessments of individual FIs and DNFBPs. There is not enough focus on

[18] For more details on the sanctions please see IO.3

ensuring that the objectives and policies of the Czech authorities are consistent with the identified ML/FT risks.

116. The LEAs seemed to be aware of the findings of the NRA and of the NSA. Although these findings led to a number of important reforms (e.g. introduction of compulsory confiscation of proceeds of crime and other amendments concerning confiscation; change of the ML offence definition; setting up of "Tax Cobra" teams[19], etc.), during the interviews held on-site, the LEAs could not demonstrate how they prioritise their cases to address particular risks identified in the NRA (for example corruption related ML cases).

117. To address the risks posed by complex corporate structures, positive initiatives have been and are being introduced by Czech Republic. Starting 1 January 2018 the Register on Beneficial Owners and the Central Register of Bank Accounts were established to improve transparency of beneficial owners and to provide quicker access to bank account information.

National coordination and cooperation

118. As the relevant legislation foresees (see also R.1), the FAU coordinates the NRA process. This includes the assessment of risks, discussion, delivery and dissemination of the final NRA report. In total, the NRA coordination meetings involve around 50 professionals from different public institutions and the private sector (see also paragraph 126). The fact that the NRA was adopted by the Government makes it a binding document for all these interlocutors involved in the AML/CFT matters. Consequently, measures listed in its Chapter 4.1 are considered binding for any entities identified as an 'implementing entity'.

119. On the other hand, it appears that coordination and monitoring of the implementation of the mitigating measures, including also the updates on the emerging risks, are done on a less formal basis. The coordination meetings hosted by the FAU to discuss the NRA updates and implementation of the mitigating measures are held regularly. However, no clear terms of reference are set, nor are official records of the discussions consistently kept. The authorities advised that these meetings were open to all those involved in the NRA process, and lately they also attracted participation from some state institutions and the private sector which were not directly involved in the NRA process. The authorities also consider that these meetings strongly influenced the understanding and awareness of risks by different interlocutors and especially by different SRBs. The conclusions of the meetings are sometimes sent to relevant institutions in the form of official communications. Despite these efforts, the assessment team considers that such meetings, including the membership in this coordination group should be formalised and clearly defined. Also, the discretion in deciding whether or not to keep a record of the meeting and when and what to communicate to the relevant authorities poses a significant risk that the efforts invested in updating the threats, vulnerabilities, state of play of mitigating measures or any other related matter may be lost.

120. Adequate monitoring of the implementation of the Action Plan (i.e. Chapter 4.1 of the NRA), in the opinion of the assessment team, might also be an issue of concern. The authorities consider the fact that the NRA was adopted by the Government as sufficient to have it properly applied in practice. This means that the implementation of the measures is a direct responsibility of the entities assigned to execute them. Consequently, non-application of a measure within the time frame foreseen would indicate a violation/non-implementation of the Government's decision. The assessment team is of the view that such an approach might not be sufficient for accurate assessment and analysis of implementation of the Action Plan. Assigning

[19] Please see IO.8 for further explanation of Tax Cobra teams.

an entity or inter-agency working group to formally responsible for monitoring the implementation of the mitigating measures and drafting periodic reports would produce better oversight. This is confirmed by the fact that, thus far, there is no report which would assess both the quality and quantity of measures implemented.

121. On the other hand, coordination and cooperation of relevant authorities in pursuing ML/FT related cases appears to be effective. The FAU has entered into agreements with many national counterparts such us Police, Intelligence Services, National Security Council, Customs Administration and Tax Directorate. Apart from these agreements, actual cooperation and coordination on both formal and informal levels was considered by all interlocutors met on-site to be one of the strengths of the Czech AML/CFT regime.

122. Apart from effective multi-agency cooperation at the national level, the Czech authorities have also regularly participated in the multinational joint investigative teams. So far, 54 such teams included representatives from the Czech Republic. These representatives always, ex officio, submit relevant information about JIT investigation(s) which is subsequently shared with their peers. As a result, numerous trainings were organised to discuss challenges in this sector and the manual on international cooperation with regard to seizures and confiscation of the proceeds of crime was developed.

123. The FAU conducted outreach with the NPO sector with regard to the prevention of FT, and the dialogue with SRBs (such as chambers of the legal profession), sector regulators (such as MoJ and MoF) and the private sector (mostly by the FAU's analytical department) have been significantly intensified.

124. The CNB also coordinates the parts of the Action Plan (i.e. Chapter 4.1) implementation through distribution of tasks to its departments in charge whilst the heads of these departments are accountable for implementation of the measures assigned to them. The CNB closely and continuously cooperates and exchanges information with the FAU. The main emphasis is on coordination of planning AML/CFT supervision and performance of on-site inspections. In 2015 and 2017 the CNB and the FAU carried out joint AML/CFT on-site inspections in two financial institutions. The CNB is also active in the legislative field, as it provides comments and suggestions to the AML/CFT draft legislation and guidelines produced by the FAU.

125. The Ministry of Industry and Trade is a coordinating body for implementation of the international control regimes with regard to proliferation. In 2006 the FAU, as a national coordinator of implementation of international sanctions set up an Inter-institutional Open Informal Working Group (IOIWG) to ensure prompt and direct cooperation and coordination among all public stakeholders on implementation of all international sanctions including those related to FT and PF. This informal platform is composed of the representatives of the FAU, the Ministry of Foreign Affairs, the Ministry of Interior and intelligence services, the General Customs Directorate, the Ministry of Education, Youth and Sports, the Ministry of Industry and Trade, the State Office for Nuclear Safety and the Ministry of Transport. The IOIWG meets quarterly and on an *ad hoc* basis as required. Nonetheless, the IOIWG has not yet considered extending its scope of operations to e.g. develop or adopt any policy guidelines in this area. The assessment team deems that the authorities might consider adopting terms of reference of this group in order to further foster the prevention of PF.

Private sector's awareness of risks

126. The private sector was involved in the NRA process in advanced drafting stages, being required to provide input on the sections of the report corresponding to their area of activity. The authorities underlined that the consultations with the private sector were geared towards

identifying potential discrepancies in the report and capturing the perception of risk rather than using them initially in the risk identification process.

127. As already noted, after the formal approval of the NRA report, the FAU produced 12 non-public tailor-made or bespoke versions, which corresponded to specific segments of the private sector. These versions were distributed by the FAU to selected obliged entities in the first wave. In the second wave FAU produced and distributed tailor-made versions for each and every segment of obliged entities.

128. The representatives of banks met on-site showed a proactive approach to risk, and demonstrated a broad understanding in this regard. Banks do not use the Czech NRA as the only source of their risk analysis, but also consider the EU Supra National Risk Assessment, public sources, their own experience, and group-wide assessments. They identified product-related risk (*e.g.* mortgage, credit loans, letters of credit), customer-related risks (*e.g.* non-resident customers, PEPs) and transaction-related risks based on potential predicates typologies (*e.g.* tax evasion, frauds, phishing schemes).

129. Insurers were focused on the client's profile in their risk assessment (country of origin, whether PEPs or not, field of operation for corporate customers). Other FIs (capital market participants and the currency exchange bureau) appeared to have a rather formalistic approach to the NRA, without a deep understanding of relevant circumstances and materiality. The focus was more related to the risk of fraud which would damage the business rather than on ML/FT threats and vulnerabilities. However, during the on-site interviews, sector-specific risks emerged which were not captured under the NRA.

130. The knowledge and understanding of AML/CFT risks by DNFBPs varies. Casinos seem to be aware of the particular risks (e.g. PEPs), but limited mitigation measures are taken. Other DNFBPs have difficulties in accepting the findings of the NRA where vulnerabilities related to their profession are identified. This negatively impacts the application of effective mitigation measures. Auditors, accountants and notaries are the most knowledgeable categories on AML/CFT risks and obligations, together with some auditing companies which develop a line of business in providing AML/CFT compliance consultancy. Real estate agents' understanding of ML/FT risks is an area for improvement.

131. As discussed above, under the "Country's understanding of its ML/FT risks" sub-chapter, the manner in which the NRA report presents the results of the risk classification needs improvement, as a number of different scales are used. Thus, it's not fully clear for the users what are the main ML/FT risks for the country. Another difficulty for the private sector is the structure and the presentation of the NRA itself: a very large document, lacking an executive summary or a condensed, concluding version. Small FIs and the DNFBPs are lacking the capacity to analyse, extract and understand the relevant parts of the NRA in order to adapt their AML/CFT measures to the identified risks.

Conclusion

132. The Czech Republic authorities have made significant efforts to understand the country's main ML/FT risks. The NRA process, which was a multi-stakeholder exercise, was conducted very diligently and transparently, backed by political commitment at the highest level. Since the NRA report did not provide any "final" or "consolidated" ranking of identified risks the assessment team believes that the specific levels and prioritisation of different categories of risks in NRA report could have been expressed in a clearer and more user-friendly manner in order to help the reader to easily establish the priorities as between different risk areas. Also the

NSA analysis was not fully integrated with the NRA, especially concerning areas related to terrorism, terrorism financing and organised crime.

133. There are areas which were not considered in sufficient depth in the NRA, such as ML/FT threats related to the context and geographic situation of the Czech Republic; the risk related to human, financial, and other resources of competent authorities; risks and vulnerabilities in respect of the use of instruments of fictitious entrepreneurships in the country; the vulnerability of the real estate sector for integration of foreign criminal assets, etc. The assessment team also takes the view that the threat of the laundering of foreign proceeds was significantly underestimated in the NRA.

134. **Overall, the Czech Republic has achieved a moderate level of effectiveness for Immediate Outcome 1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6 (Financial Intelligence and Other Relevant Information)

- The FAU accesses and obtains information from a broad range of databases containing financial, administrative and law enforcement components. The FAU also receives, upon request, additional information from any public authority or reporting entity, regardless of whether such entity previously submitted a STR. In general, the quality of the information contained in the databases is adequate, whilst certain concerns remain with the accuracy of the real estate and commercial registers. In case of indirect access, authorities provide the FAU with information in a timely manner.

- The FAU produces good quality financial intelligence. The statistics and case examples provided confirm that this intelligence is, to a certain extent, used in ML and associated predicate offences investigations. However, the statistics do not provide a clear breakdown of use of the FAU's disseminations in initiating ML as opposed to proceeds-generating predicates.

- Limited feedback is provided to the FAU on use of financial intelligence by LEAs. This practice does not enable the FAU to adequately assess the quality of its analysis and prioritise its own course of actions.

- LEAs regularly use other information (e.g. their own intelligence, complaints from the public and information gained in the course of investigating predicate offences) to initiate ML and FT investigations. The FAU is often involved in such investigations and provides LEAs with information and expertise in a timely manner ensuring also the confidentiality of such communication.

- The FAU is in general satisfied with the quality of STRs submitted by the financial institutions, while the same cannot be stated for the quality and quantity of STRs submitted by DNFBPs. Should the FAU receive a low quality STR, it reaches out the obliged entity on the need for further improvement. At the same time there are serious concerns related to the function these SRBs, since in practice they, rather than the DNFBP concerned, make a decision whether the STR should be submitted. Deficiencies identified with respect to the definition of suspicious transactions, as well as the timeframe for submitting a STR may further hamper the proper compliance with the reporting obligations. While the NRA identified the real estate sector and legal professionals as vulnerable to ML abuse, only few STRs were submitted by these obliged entities.

- The FAU has adequate human, financial and technical resources to conduct operational analysis. However no written guidelines on STRs prioritisation are in place. With regard to strategic analysis, apart from the typologies prepared for the purposes of the NRA, there is little evidence of the FAU's efforts hereof.

Immediate Outcome 7 (ML investigation and prosecution)

- Since the previous evaluation, legislative reforms and increased efforts in pursuing ML investigations represent a clear step forward. However, more investigative opportunities should proactively be undertaken and pursued, as a significant number of such investigations are ultimately suspended, in part due to unfruitful responses from foreign jurisdictions.

- The assessors were shown some successful completed large scale ML cases, though the number of these was modest. It is encouraging to see that a greater number of serious offences are being investigated and prosecuted in recent years. However, the clear majority of these have not yet reached a final conclusion.

- Based on available information it cannot be concluded that the focus of ML investigations and prosecutions is fully in line with the central ML risks for the country in terms of underlying criminal activity, though other information generally confirms a correspondence between them. Too often, it would appear that the ML investigation is merely tagging along on the predicate offence(s) investigation.

- Serious large scale third party and stand-alone ML investigations, prosecutions and convictions continue to be the exception. A good number of investigations are based on a predicate offence committed abroad.

- The prevalent practice within the Czech justice system of sanctioning multiple offences simultaneously makes it difficult to measure the precise impact of the sentence in relation to ML. Nevertheless, in certain cases where ML was prosecuted in the absence of the predicate, dissuasive and proportionate sentences were in fact obtained.

- In certain fraud related ML cases where a conviction cannot be obtained (e.g. the perpetrator is unknown or outside the CzR), the authorities have nonetheless been able to make restitution of the property to victims. In a limited number of cases, confiscation is obtained where a ML conviction is beyond reach. In addition, specific tools are available in the tax legislation which enable the recovery of funds that constitute an illicit gain.

Immediate Outcome 8 (Confiscation)

- The assessors acknowledge the improvements in the legislative and institutional framework (e.g. access to relevant databases and introduction of the 'extended confiscation'[20]). That seizure and confiscation represent policy priorities for authorities is clear.

- Based on the statistics presented, the amounts confiscated for the period, although still far inferior to those seized and frozen, are nonetheless significant. Amounts that have been frozen may still be confiscated but during the period under review many of the relevant cases were still pending.

- LEAs regularly carry out financial investigations in relation to proceeds-generating offences confirming their effectiveness in terms of significant results with respect to seized and confiscated assets. There is an increasing specialisation in the area of financial investigation (at LEA and judicial levels) and external expertise is available upon request.

- Little information was provided to demonstrate effective results with respect to undeclared cross border transportation of cash and bearer negotiable instruments.

- Data presented to the assessment team confirm that seizures and confiscation are largely related to the primary offences constituting ML risks.

[20] Extended confiscation is a term used to reflect the ability to confiscate assets (in criminal proceedings) that go beyond the direct proceeds of a concrete criminal offence for which the defendant is prosecuted. The scope of the extended confiscation then goes to all the assets that are suspected to be proceeds of crime unless the defendant can prove their legal origin. The 'extended confiscation' notion is also included in the FATF Best Practices Paper on Confiscation (pg.6, par.17) whilst it became a part of the EU Directive 2014/42.

- The asset management system, aimed at preserving the value of the seized assets, appears to be complete and functional. In addition, the country demonstrated, through examples, the ability to share the confiscated assets with foreign jurisdictions.

Recommended Actions

IO.6:

- LEAs should use the financial intelligence provided by the FAU more proactively to investigate ML cases independently and not only when targeting the underlying criminal activity.

- LEAs should regularly provide detailed and adequate feedback to the FAU on the quality of their dissemination and their further use, indicating the type of criminal activity information is used for.

- Authorities should ensure that the role of SRBs with regard to STR submission by some of the DNFBPs (e.g. accountants, lawyers, notaries) is limited to formal checks as the legislation provides[21]. Authorities should consider whether the SRBs' intermediary role in the STR reporting is justified.

- Written guidelines and specific indicators on STR prioritisation should be prepared and enforced by the FAU's analytical department.

- The FAU's strategic analysis should be further enhanced with a view to: i) better inform AML/CFT risks and policies; ii) identify trends and typologies; iii) serve LEAs to detect and investigate ML, associated predicate offences and FT.

- Technical deficiencies in relation to the definition of suspicious transactions, as well as the timeframe for submitting an STR by lawyers, tax advisors, notaries, bailiffs and auditors should be rectified.

- Authorities should take measures to ensure that the information kept in the real estate database and the commercial registers is accurate and up-to-date.

IO.7:

- Czech authorities should focus more efforts and, as required devote greater resources to large scale and complex ML prosecutions that more closely align with the identified risk predicates;

- CzR authorities should find ways, including as required through legislative amendment, to streamline the pre-trial and trial process in order to shorten the average length of prosecutions in serious ML cases;

- In order to ensure prioritisation of ML investigations and prosecutions, CzR authorities should continue to strengthen specialised units and regularly re-evaluate whether they have sufficient resources to deal with the country's risks;

- CzR authorities should consider amending ML offence so that it does not require in all cases a clear identification of the predicate, but merely sufficient evidence to show that one or more criminal offences underlie the assets in question;

- In order to increase the number of ML charges and prosecutions CzR authorities should continue to further train investigators in relation to financial investigations.

[21] This recommendation is also relevant for IO.4.

IO.8:

Czech authorities should:

- carry out periodically a stock taking exercise on effectiveness and impact of the recently introduced NBC and extended confiscation mechanisms as well as on the use of recently created BO and Central Bank accounts registers. Based on the results of these periodic exercises the appropriate measures should be included in the updated NRA and Strategy to Combat Organised Crime;
- find ways, including as required through legislative amendment, to streamline the pre-trial and trial process in order to shorten the average length of prosecutions in cases which involve confiscation of proceeds of crime.
- strengthen the capacities of the relevant authorities in the area of cross-border control of cash and BNI so that they can better identify and investigate suspicious of ML/FT. LEAs should be given a mechanism to freeze the cash whose origin is unknown. The authorities are also recommended to develop a guideline for detecting cash smugglers which would include indicators on profiling of those involved in such activity.
- consider whether AMO's role should be extended so that they play an active part not only in managing the assets seized but also in executing the confiscation orders.
- maintain more detailed statistics on the amounts and nature of property seized, frozen and confiscated. This should include incoming and outgoing MLA requests for seizure and confiscation.

Immediate Outcome 6 (Financial intelligence ML/TF)

Use of financial intelligence and other information

a) Access

135. The FAU and LEAs have access to a wide range of information held by the private sector and relevant authorities. The FAU has access (direct or indirect) to a broad range of databases containing financial, administrative and law enforcement information. In case of indirect access, information is provided in a timely manner. Information contained in the Police databases is provided within hours, whilst other types of information obtained indirectly the FAU receives it within a week, if there is no need for an urgent response.

Table 3. FAU Access to Non-public Databases

Resource manager/ provider	D (database) CH (channel) S (Information Source) T (tool/application)	Type of access: A (automatic access) M (manual access)	Available information
CA (MoF)	D	A,M	Database of declarations of cross-border transactions
MoI	D,S	M	Register of Vehicles (vehicle registration plates, vehicle owner, vin code etc.)
MoI	D,S	A,M	UNIQUE-CEO (Register of persons, relatives etc.)
Police, MoI	S	M	Police database information
NSA	D	M	Register of National Security Authority

MoF	S	A,M	ARES internal register of economic subjects (legal, natural persons), including special ID - personal identification number.
MoF	S, CH	M	VIES - VAT validation
TA, MoF	D	A,M	ADIS DS (tax arrears, tax returns, risk factors of tax subjects etc.), register of VAT payers
Chamber of Bailiffs	D	M	Register of executions
Czech Office for Surveying, Mapping and Cadastre	D,S	A,M	Land Property Register
Bisnode, FIU Czech rep.; CRIF, FAU	D	A,M	Magnus in-house database, Cribis in-house web and a database (business information on Czech and Slovak companies)
Central Register of Bank Accounts	D	A	Bank account information

136. The FAU can request additional information from any public authority or obliged entity. Information is obtained from obliged entities regardless of whether they had previously submitted a STR. In general, the FAU is satisfied with the quality and completeness of the information available via databases whilst concerns remain with the accuracy and completeness of the real estate register and the Commercial register of the legal entities' basic and beneficial ownership information. These two databases are of particular concern in light of the ML/FT risks posed by the real estate sector and by the misuse of the legal entities. Further analysis of the risks related to these matters is reflected in IO 1 and IO 5.

137. The Central Register of Bank Accounts has been set up to facilitate access to bank accounts information. The Register is fully populated and is operational since 1 January 2018. The FAU, intelligence services, tax and customs administration and prosecutors have direct access to the Register whilst police need a prosecutor's approval (s. 6 of the Act on Central Register of Bank Accounts) to access this database. The Register is frequently used, and so far there have been 6 624[22] requests for access made by the competent authorities. However, it is still too early to determine precisely the extent to which this database assisted the authorities to better perform their analytical and investigatory activities.

Statistical data on requests to the Central Register of Bank Accounts	
Total amount of received requests	6 624
Total amount of processed requests	6 624
Average time of request processing [minutes: seconds]	*16:57*
Number of requests from courts (Sec. 7 para. 3a)	8
Number of requests from public prosecutors (Sec. 7 para. 3b)	2 532
Number of requests from body authorised to receive suspicious transaction reports (Sec. 7 para. 3c)	2 785
Number of requests from Security Information Service and Office for Foreign relations and Information (Sec. 7 para. 3d)	0
Number of requests from Military Intelligence (Sec. 7 para. 3e)	0
Number of requests from Tax Administration (Sec. 7 para. 3f)	1 213
Number of requests from Customs Administration (Sec. 7 para. 3 g)	86

[22] Statistics are available at: https://apl.cnb.cz/ceuweb/ceuweb.ceuw_forms.zprava

Other service data on Central Register of Bank Accounts	
Total number of records in the system	39 933 694
Daily average increment in the system	72 264
Number of accounts which are subjects to the system	27 025 202

b) Use

138. Financial intelligence and other information is used to a certain extent by the competent authorities to investigate ML and associated predicate offences. The results of FAU analysis are disseminated to the LEAs either in the form of a criminal complaint[23] or as information that they could use for the purposes of their pre-existing investigative activities. The financial intelligence can be provided to LEAs spontaneously and upon request.

139. As provided in the Table 4 below, over the last 4 years the FAU disseminated 2306 criminal complaints to the LEAs. Authorities indicated that majority of disseminations contain a hypothesis of ML in conjunction with the predicate offence. Approximately 1/5 of the criminal complaints contain a hypothesis of a predicate offence only, and some of stand-alone ML. Overall, the majority of criminal complaints submitted by the FAU is based on STRs. The other part is based on the analyses the FAU carried out upon information received from other authorities, foreign counterparts, media and their own research. According to the partial statistics provided to the assessment team, around 30% of the FAU criminal complaints triggered criminal instigation. Although the LEAs confirmed that the FAU disseminations are very important for initiating ML related criminal proceedings, they advised that in practice these disseminations are largely used for investigating predicate offences.

Table 4. Use of financial intelligence for investigation of criminal cases

Year	Criminal complaints from the FAU to LEAs, of which on			Suspension of funds	Criminal cases instigated, of which on	
	ML (criminal complaints on ML with indication of predicate offence)	Stand-alone ML	FT	No. of times this measure was applied as per crim. complaint	ML offence solely or concurrently with predicate offence	FT
2014	680	Not available (N/A)	0	263	144	0
2015	514	N/A	0	294	115	0
2016	556	N/A	0	402	192	0
2017	539	17	0	377	227	0
Total	**2289**	**17**	**0**	**1336**	**678**	**0**

140. With regard to the types of predicate crimes, no exact breakdown per criminal complaints appears to be available. Nonetheless, both the FAU and LEAs confirmed that the most common predicates were tax offences, various forms of frauds (from simple types of fraud to those highly sophisticated such as credit and subsidy frauds), phishing/pharming, tax offences, false bankruptcy, corruption and drugs trafficking. This is further confirmed in the FAU annual reports. In general, the intelligence gathered and criminal complaints submitted by the FAU correspond to the NRA findings on most common ML predicates indicated thereof. The

[23] Criminal complaint is a document/report (S. 159 of the CPC) that sets forth the basis upon which a criminal proceedings may be initiated. The standard is reasonable suspicion: person is to be charged with an offense.

assessment team was presented with a number of cases demonstrating the extensive use of FAU intelligence by LEAs, some of them being included also in the IOs 7 and 8.

Case example 1: A criminal case initiated by the FAU based on a STR (tax fraud)

Based on the information provided via STR, the FAU analyses revealed a network of companies involved in VAT related carousel fraud. The FAU identified individuals from these companies who were behind these activities and prepared their ML risk profiles. Fictitious services with transactions involving fictitious goods were the main criminal activity. Once the FAU prepared the risk profiles of the suspects and analysed the transactions conducted, they communicated with NOCA and the COBRA team before filing a criminal complaint. Further to information exchange, the FAU submitted the criminal complaint which identified that the approximate amount of damage was about EUR 4 – 6 million. Subsequently the seizure request was filed by NOCA and EUR 4 million were frozen. The investigation is still underway.

The FAU advised that their active role in pursuing the funds identified as fraudulent and their assistance provided to Police in executing the freezing order was of paramount importance in this case. In other words their action did not end with simple analysis of the suspicious transaction and its dissemination, but in numerous other activities which police afterwards built on to enable freezing and the continuation of criminal investigation.

Case example 2: A criminal case initiated by the FAU based on a STR (ML)

With the aim to illegally trade in narcotics the perpetrator created e-shop (as a part of the autonomous network TOR) accepting virtual currency – bitcoin (BTC). He charged a commission of 0,038 BTC for each transaction. By misusing the private keys of a bitcoin wallet of the e-shop he took 840 BTC.

The perpetrator´s wife changed, in the "bitcoin exchange office", about 802 BTC acquired by her husband and subsequently transferred funds in the amount of EUR 200.000 - to her and her husband´s accounts. Analysis by the bank confirmed that prior to that the same account had been credited with a payment of EUR 35.950 - from a company providing services with virtual currency. The bank initiated an enhanced CDD and blocked the funds. The suspects explained that these funds were acquired through the purchase and subsequent sale of BTC. Further checks confirmed that there was no evidence of trade in BTC in the period referred by the owner of the account. The FAU blocked the amount of EUR 35.950 - and filed a criminal complaint including information about serious suspicion of committing a criminal offence of legitimization of proceeds of crime (i.e. ML). The IT expertise by the FAU and LEAs enabled the seizure of BTC. In addition, the seizure included, EUR 200.000 - 2 real estate properties in the value of EUR 480.000 - 4 luxury vehicles in the value of EUR 208.000 - and electronic devices in the value of EUR 60.000. The main perpetrator was accused for production and trafficking in narcotics and theft, while his wife was charged for ML. The case is still before the court.

141. Communication between LEAs and the FAU is smooth and prompt. LEAs actively request financial intelligence from the FAU when conducting investigations on ML and associated predicate offences. Over the period 2014-2017 the FAU received 1178 information requests from LEAs (263 in 2014; 261 in 2015; 248 in 2016; and 406 in 2017). A mere indication of ML, which LEAs come across, is sufficient for the FAU to initiate the analysis, submit it to LEAs and engage further if need be. Authorities advised that so far they have not experienced any impediments where this type of cooperation is concerned leading to a conclusion that the technical deficiencies identified in relation to C. 29.5 do not have an impact on the effectiveness of the FAU operations in practice.

Case example 3: ML and predicate offence investigation initiated by LEAs

The Police investigated the criminal activities of 4 persons concerning unauthorised production of methamphetamine and its subsequent sale. The financial investigation was focused on the main perpetrator and members of his family. The FAU was requested to analyse the bank accounts of suspects

and the consistency of the transactions with the account owners' profiles. One of the suspects (a woman on maternity leave) deposited in cash (during 15-month period) an amount of EUR 605.926. Approximately one third of this amount was transferred to a savings account whilst the rest was transferred to several different accounts or withdrawn in cash. There was no proper justification of the source of funds, nor a proper explanation for these transactions. Within the framework of a house search the Police also seized EUR 220.000. The main perpetrator was convicted of unauthorised production and trafficking of narcotic, psychotropic substances and poisons and was sentenced to 9 years. His girlfriend was convicted for ML and received 3 years suspended sentence. The funds were confiscated.

142. Cooperation between the FAU and Tax Administration appears to be an appropriate response to the fact that tax crimes, including tax evasion and carousel fraud, are considered as major threat for ML. The FAU disseminations are sent to Tax Administration in the form of informative letters. During the period 2014-2017, the FAU has sent 6301 informative letters to the Tax Authorities. Any suspicion on tax related crime is communicated immediately to the Tax Administration and LEAs. The FAU regularly informs the Tax Administration on the freezing of funds in cases of suspicion of tax evasion. Further cooperation in investigating tax related crimes is executed within the framework of so called 'COBRA' investigative teams[24]. Although the FAU is not directly included in these teams, it provides them with expertise and analysis of financial flows. However, from the interviews held on-site, the assessment team noted that in practice, it had happened that the Police was the sole recipient of information on tax frauds. Nonetheless, it does not necessarily indicate any negative impact on the effectiveness of these criminal investigations.

Case example 4: A criminal case investigated by the Police and the Tax Authorities with the support of the FAU (Tax evasion and ML)

In order to obtain unlawful excessive deduction of VAT, the perpetrators created a network of inter-connected companies. Their main "business activity" was to issue false invoices for simulated services to be used for illegal reduction of income tax. For the purpose of money laundering the perpetrators used bank accounts of these companies - for example one of the main perpetrators, in his capacity as a member of a statutory body of a company, set up 5 bank accounts in the Czech Republic. The amounts were then transferred to these accounts and collected in cash. The FAU analytical work and cooperation with the Tax Administration and Police resulted in the successful completion of the investigation. Consequently, the court convicted 5 persons for tax evasion and 4 persons for ML. The sentences ranged from 4 and 7 years imprisonment, whilst the funds EUR 640.000 were confiscated together with the fine amounting to EUR 110.000.

143. The FAU proactively seeks intelligence from the foreign counterparts to further support its financial intelligence analyses and investigations initiated by LEAs. Given the risks and context of the country, the active role by the FAU and LEAs and efforts they invest to obtain information from abroad are of significant importance in pursuing ML related predicate offences and FT. Case studies presented in the report (i.e. the case below but also 'CEO Fraud' and 'Corruption' cases under IO7) further support this conclusion. The only impediment noted so far by the Czech authorities with regard to international cooperation in this context concerns timeliness in obtaining information from some off-shore jurisdictions (see also IO.8).

Case example 5: A criminal case initiated by LEAs using information requested form the foreign FAU (Corruption)

[24] For more details on 'Cobra' cooperation platform please see IO.8.

The Unit for Combatting Corruption and Financial Crime of the Czech Police investigated several persons in relation with the offences of breaching their duty in the administration of property, arranging advantage in commission of public contracts and accepting bribes.

With regard to the granting of the public contract and manipulations committed in relation thereto, the Police found that the persons concerned had set up corporations in order to launder the proceeds of crime. For the purpose of hiding the beneficial owner of the proceeds, the suspects used the bearer's check (*note: bearers checks are not in use in CzR as of 2014)*. The acquired proceed of crime, in the value more than EUR 2,120.000 after being transferred abroad to the accounts of these corporations were then withdrawn in cash – both at the bank counter and in ATMs. Once withdrawn, the cash was distributed to other suspects. For this complex investigation, smooth cooperation had to be ensured not only at the domestic but also at the international level. In agreement with LEAs, the FAU requested and obtained additional information from their foreign counterparts. Consequently, the FAU sent requests to several FIUs (Cyprus, Liechtenstein, Marshall Islands, Hong Kong, Seychelles, Switzerland, Austria, etc.) whilst FinCEN (US), in cooperation with the FBI, also provided relevant information. The case is still before the court.

144. With regard to ML investigations triggered by LEAs using information other than the FAU's disseminations (please see Table 6 under IO7), it has to be noted that LEAs initiate such investigations based on their own intelligence information, complaints from the public (e.g. frauds and phishing being usually the predicates) and information gained in the course of investigating predicate offences. The majority of the cases presented to the assessment team suggests that this 'other than the FAU generated information' is mostly used to pursue predicate offences and associated ML. In other words, cases of autonomous ML resulting from investigations initiated by LEAs are rather rare.

145. The FAU confirmed that it had received information on FT suspicion from reporting entities, foreign counterparts and from the intelligence services. FT suspicions received from the reporting entities were related to partial matches with designated persons under the TFS regime. Information on the FT suspicions received from the foreign authorities mostly concerned flash reports that countries disseminate to foreign jurisdictions requesting information on persons designated in their national lists. As for the information received from the intelligence services, the Czech authorities could not share the details with the assessment team due to confidentiality reasons. In any event, a FT suspicion, no matter from which source, is analysed by the FAU as a matter of priority. Further, the FAU then discusses its findings with LEAs in face-to-face meetings. However, the FAU analysis and their further examinations with LEAs did not confirm that FT occurred in any of these cases.

Reports received and requested by competent authorities

146. The FAU receives STRs from the reporting entities, information on suspicion of ML/FT from Tax and Customs Administrations and foreign FIUs, reports from intelligence services and other relevant authorities (e.g. supervisors). Overall, the FAU is satisfied with the quality of STRs submitted by the obliged entities. About 1/4 of the STRs result in criminal complaints that the FAU submits to LEAs.

147. The FAU receives a high number of STRs, the volume of which is growing from year to year. From 2014 to 30 June 2017, the FAU received more than 13 000 STRs. These STRs mainly concern the suspicion of ML and predicate offences. Very few STRs were received on FT. These reports were mostly submitted by the banking sector, and in one case – by the bureau de change, and based on a partial match with the different sanctions lists (see also IO 10).

148. The vast majority of STRs were submitted by banks and other financial institutions. At the same time, the volume of reports received from the DNFBPs remains low (please see Table 13 and paragraph 421 under IO.4). As indicated by the FAU the DNFBP sector should improve the quality and the quantity of reports. The key reasons for such practice lies in the lack of awareness and guidance on STR reporting for the non-financial sector. In addition, Section 6 of the AML Act provides a list of 12 indicators for submitting STRs, most of which are, however, relevant for the financial sector only. Taking into account the fact that DNFBPs tend to rely on this list of indicators, a suspicious activity falling out of the scope of these indicators may be disregarded. The NRA notes that the majority of ML related vulnerabilities stand with the financial sector and therefore the frequent reporting of suspicious transactions by this sector is, in general, in line with the country's risk profile. Whilst the NRA notes that the DNFBPs are also vulnerable to ML/FT threats, only few STRs were submitted by the sector.

149. STRs from the financial institutions are submitted directly to the FAU through the MoneyWeb secured electronic connection. Other obliged entities are given access to MoneyWeb Lite Client, however their STRs are submitted via databox, e-mail or are handed over to the FAU in a paper form. Nonetheless, the number of STRs submitted in paper form is negligible, i.e. less than 1% of total STRs submitted.

150. Some DNFBPs submit STRs through their self-regulatory bodies (SRBs). Notaries, lawyers, tax advisors, bailiffs and auditors send their suspicious transaction reports to the respective chambers, which then conduct further checks. Whilst the law imposes that these chambers check "if the STR includes all requirements stipulated in the AML/CFT Act" the understanding of the FAU is that these checks are limited to rather formal completion of the STR template. However, meetings held with the aforementioned DNFBPs and their SRBs indicated that these checks extend further to the analysis of substance included in these forms. Based on this analysis the SRBs decide whether a STR should be submitted to the FAU. As a matter of fact, it was noted that SRBs provide no information to the FAU on STRs which they did not file based on their own decision. This raises serious concerns if the role of these SRBs goes beyond what the respective legal provision provides. In addition, whenever the FAU seeks additional information from these obliged entities, the communication is carried out through the respective SRBs. In any event such a practice negatively impacts the ability of these DNFBPs to execute their obligations with regard to identification and submission of information related to suspicious transactions/activities. Such a practice may also increase the risk of confidentiality breaches and may prolong the period between the point when the STR is submitted and the moment suspicion was identified. On the other hand, filtering the suspicious transactions reporting through the relevant SRBs can prevent defensive/over-reporting by DNFBPs.

151. Although no statistics are available with regard to requests the FAU made to the reporting entities following the submission of the STRs their communication on this matter is intensive. The obliged entities almost always consult the FAU prior to submitting a STR. These consultations are twofold: they either aim at i) providing advice and guidance to the DNFBPs who have limited experience with STRs preparation and submission, or ii) include discussions on complex chains of transactions where the reporting entity seeks advice to better prepare the STR and include all relevant info therein. The evaluation team considers this a positive practice – it ensures continuous education of the REs and a prompt feedback on cases.

152. In addition to the meetings held on an individual basis, a number of trainings were organised for the reporting entities on their AML/CFT obligations. Although the FAU noted an increase of quality of the STRs filed, written guidelines for the obliged entities which would, inter alia, include suspicious transactions indicators would certainly be an asset in this process.

153. Apart from the STRs, the FAU receives information on possible ML from Tax and Customs Authorities via MoneyWeb. In the light of the risks identified in the country, the number of reports submitted to the FAU seems to be adequate. However, only 15% of these reports have resulted in criminal complaints. Moreover, no information has been provided to the assessment team on further use of these complaints by the LEAs, thus the effectiveness of the latter cannot be assessed. Information on cross-border cash declarations, as well as on falsely declared or not declared cash is submitted to the FAU on a daily basis. In case the Customs Authority has any suspicion related to the origin or intended use of money, they indicate this to the FAU. It needs to be noted that the Customs Authority applies a cumulative approach with regard to the amount transported during one year period: if over a 12 month period the amount of cash transported by the same person exceeds EUR 10,000 threshold, then it has to be declared. In the absence of comprehensive statistics it remains unclear how often this information is used by the FAU for its analysis, how useful it is and whether it has contributed to the initiation of a criminal complaint.

154. As already noted, the FAU also receives FT related information from the intelligence services. Although the FAU advised that this information is a very useful source for their analysis, neither statistics nor case studies were presented given the confidentiality clause.

Operational needs supported by FIU analysis and dissemination

155. On 1 January 2017, the FAU became autonomous from the Ministry of Finance. It now acts as an independent national centre for receiving and analysing suspicious transaction reports and for dissemination of the results of the analysis. The FAU submits annual report on activities to the Government. Selection, appointment and dismissal of the director and the personnel of the FAU are regulated by the Act on State Service. The evaluation team noted that the reorganisation of the FAU resulted in the increase of its resources and analytical capacities.

156. The FAU now has 56 staff members, 35 of which are responsible for operational and strategic analysis, while the rest of the team is in charge of legal compliance, international cooperation and IT. The FAU staff is regularly trained on various aspects of their work, including (but not being limited to): AML/CFT legislation developments in domestic and international levels; confidentiality and data protection in the FAU activities; reporting entities and their risk assessments; usage of FAU's databases and IT tools; specific features of the FAU's cooperation with police, Tax and Customs Administration, etc. Apart from these, the FAU's staff is also involved in other trainings organised in cooperation with its national and international counterparts. There is a proper clearance level for the FIU staff. Most of the analysts working in the FAU are former police officers.

Operational analysis and dissemination

157. Whenever a STR is received, the Head of Analytical Division assigns it to one of the analysts based on his/her expertise in relation to the financial flows from the alleged predicate offence. The FAU's analytical work is run 24/7 including weekends. The receipt of a STR always triggers the opening of a case.

158. The priority is given to the STRs upon which the transaction(s) is suspended (these usually include large amounts) and those that include FT suspicious. According to the *"FAU director's instruction adjusting the process of STR analyses*", the time limit for operational analysis is 60 days and this limit could be prolonged with the consent of the Director of the Analytical Department. There are no written guidelines for STRs prioritisation developed by the FAU. The fact that there are no precise rules in place for prioritisation of STRs, together with the afore-mentioned timeframe for operational analysis, as well as the rapidly growing number of reports

received, raises concerns and can impact the FAUs ability to duly approach and analyse the whole amount of STRs.

159. Regarding the IT resources, the FAU uses custom-made ELO and TOVEK databases to manage its cases. During the onsite visit these tools were temporarily out of use, thus the evaluation team could not assess to what extent they support the FAU's analytical work. In addition, the FAU uses the "Superúčty SUPERACCOUNTS" software to extract and structure bank statements data, and ARES DWH software for visualization and analysis data.

160. The FAU seeks additional information once their analysis of the STR is underway. Their outreach usually goes beyond the obliged entity which submitted STRs and includes communication with all those who might have some links with the transactions under scrutiny.

With regard to the scope of the FAU powers, the evaluation team was provided with an inconsistent interpretation – i.e. whether an analysis on criminal activity which has no indication of ML falls within their scope of activities. Whilst the FAU advised that it can analyse any criminal activity, the statistics presented (Table 4) suggest that the FAU criminal complaints always contain an indication of ML.

161. The FAU analyses revealed different ML techniques used by the launderers, which inter alia, include i) repeated transfers between the banks in Czech Republic and abroad (including to and from shell companies established to conceal the origin of assets); ii) use of financial market products (loans, framework credit agreements, mortgages, redemption and trading of receivables, investment tools, securities) for ML purposes; iii) abuse of bank accounts set up by using fake or stolen identity; iv) use of fake consultancy or other services or goods to conceal the origin of funds; v) trade in real estate or in virtual currencies to legalise proceeds or crime; and vii) cash withdrawals of funds obtained through frauds or phishing schemes. Numerous case examples presented to the assessment team (and some of them described under IO6 and IO7) led to a conclusion that the analytical capacities of the FAU allow them to carry out the analysis of complex cases and detect different sophisticated methods criminals use to conceal or disguise the origin of illegally obtained assets.

Overpriced real estates

A company A bought from the Czech railways a property for price CZK 203.111.008 (approximately EUR 7,879,488). This property had been sold 3 years later to the Charles University for nearly double price – CZK 402.500.000 (approximately EUR 15,614,823). The Charles University paid CZK 30.000.000 - from its own budget whilst the rest (CZK 372.500.000/EUR 1,163,837) was paid by the Ministry of Education, Sports and Youth under grant system. The FAU inquiry into market prices and possibility that the value of the real estate significantly increased due to this or any other reason (e.g. significant reconstruction) could not justify such an increase of price. Circumstances of this trade raised suspicion of corruption. Further inquiries revealed a chain of false expert opinions on the market price of the real estate which were then abused by those involved in the trade. The perpetrators also used a chain of bank accounts opened in the Czech Republic and Switzerland to transfer the amounts acquired through the trade. The FAU analytical work in cooperation with LEAs led to a successful investigation which resulted in four persons being charged for providing "false expert opinion" and four persons for "fraud". At the same time three persons were accused of ML.

The Police unit seized funds in cash - in the value of CZK 775.247 (EUR 30,073), funds on a bank account in the value of CZK 59.014.042 (EUR 2,289,287) and real estates in the value of CZK 330.643.000 (EUR 12,826,383). The case is still before the court.

Autonomous ML

For the purpose of laundering proceeds of crime through account opened in Czech Republic a foreign

citizen bought ready–made Czech legal entity which had no business history. The purchase of the entity was executed through a straw man. The beneficial owner was the only one authorised to dispose the entity's funds through its account. These disposals were always executed through internet banking from abroad. The owner ordered a transfer of nearly all the amounts the legal entity received from abroad (his country of origin) to accounts opened in third countries. These transactions were rejected by the bank which also asked for additional information within the CDD process. The bank immediately submitted a STR to the FAU. Further checks revealed that documents provided in the CDD process were poor, whilst checks in databases confirmed that person controlling the entity was mentioned in Panama Papers, and in the FAU's and Police database as well. Intense cooperation with the foreign country FIU resulted in criminal complaint on ML (without indicating exact predicate) committed abroad. The funds deposited on the account of the Czech legal entity were frozen (13 304 955 USD). The criminal proceeding is still underway.

162. The number of information requests from the competent authorities to the FAU is constantly growing (see Table 5). The analyses the FAU produces are accompanied by a wide range of materials, which include: i) data on subject(s) concerned (e.g. in case of legal entity(ies) its ownership structure, scope of activity, etc.), ii) overview of bank accounts (not only accounts opened in a name of natural/legal person concerned but also these which are controlled and used by this person) and iii) various documents deriving from the CDD process, including graphs and flow-charts allowing the user to visualize relationships and possible linkages between different persons, accounts and transactions.

Table 5. Requests for information received by the FAU from national authorities

	2014	2015	2016	2017
Information requests from authorities:	***263***	***261***	***248***	***406***
Police	**252**	**240**	**235**	**388**
Customs	**11**	**21**	**13**	**18**
Tax Administration	**0**	**0**	**0**	**0**

163. When disseminating information in the form of the criminal complaint, in order to facilitate successful seizure of illicit assets, the FAU frequently applies a 3 day suspension of transactions/funds (please see Table 4). Overall, almost 2/3 of the criminal complaints submitted by the FAU included suspension order. Authorities also advised that, in approximately 80% of cases when the initial suspension was applied by the FAU, it was then followed by the seizure order by LEAs, which demonstrates a high quality of the FAUs disseminations and a prompt and effective cooperation with LEAs.

164. International cooperation constitutes an important and significant part of the FAU activities. As introduced in the Table 22 (IO2), disseminations and information requests from/to foreign counterparts were constantly growing since 2014. As confirmed through the case examples, this cooperation brought very good results in detecting complex ML schemes and tracing the illicit assets.

165. As already noted, the FAU has received very few requests from abroad which concerned the identification of assets held by persons and entities designated by the foreign jurisdictions. Further checks carried out by the FAU and the REs revealed no traces of such assets in the CzR.

166. Whilst foreign FIUs have appreciated the efforts of the FAU to produce and share good quality analyses, the FAU noted that, upon their request, some foreign FIUs did not provide

satisfactory information. This primarily concerns non-European FIUs and those which did not sign a MOU with the FAU (see IO.2).

a) Strategic analysis

167. The FAU advised that their work on NRA and typologies collected therein represent a part of its strategic analysis. The NRA includes typologies in a form of sanitized cases accompanied by i) information on types of obliged entities exposed to such *modus operandi*; ii) risk factors; and iii) suspicious indicators. Given that the typology of the predicate offence largely influences the technique of subsequent money laundering, the analyses provided in the NRA also elaborated on the interconnection between the two. As noted under IO.1, these typologies mostly concerned the laundering of proceeds deriving from tax crimes, fraud, corruption, phishing, and subvention/subsidy frauds. Some strategic analyses are also provided in the FAU annual reports. Apart from the typologies observed in the NRA and the annual reports, no other strategic analysis has been produced by the FAU. At the same time given the nature of the afore-mentioned typologies (they were developed based on the cases already investigated by LEAs), there is a little evidence that they could bring added value and be used by LEAs to better detect new trends and techniques of ML, associated predicate offences and FT.

Cooperation and exchange of information/financial intelligence

168. There are safeguards in place to protect the confidentiality of information exchange. These safeguards are provided in the AML Act and breach of confidentiality in this context is an offence punishable by the law. In addition, the authorities use secure channels of communication on the national level, such as MoneyWeb, EDOS, "Data Boxes", and ESW, FIU.net. for international cooperation.

169. Cooperation and communication among the authorities is carried out on a daily basis, through various meetings and multilateral discussions and trainings. The FAU, being an administrative type of FIU, has not been directly included in joint investigative teams in the country or abroad, but their expertise and financial analysis have always been at these teams' disposal. This was confirmed in practice through several examples presented to the assessment team and in this report (notably under IOs 2, 6 and 7).

170. Although it is not a mandatory requirement for cooperation, the FAU concluded an agreement on information exchange and cooperation with the Police, intelligence services, Tax Administration and other competent authorities.

171. The FAU is not fully aware of how the results of their disseminations are later used by LEAs. This conclusion is based on the discussions held onsite, given the incomplete statistics on this matter. From the procedural point of view, the FAU submits the criminal complaint to the Police Presidium, which later on decides which division of the Police shall further pursue the case. Acknowledgement of the receipt and any information relating to further dissemination of the criminal complaint is then sent in a form of information to the FAU. Nevertheless, as of that moment, feedback by Police to the FAU on further proceedings is optional and mostly depends on the particular police officers to whom the case was assigned. This practice does not enable the FAU to adequately assess the quality of its analysis, track the use of its criminal complaints and better inform its own course of actions. Although LEAs expressed satisfaction with the quality of information received from the FAU, the practice elaborated above does not foster the FAU's efforts to better support the operational needs of the competent authorities.

Conclusions

172. The FAU has an active role not only in analysing suspicious transactions but also in providing continually advice and expertise to LEAs on ML/FT related matters. It gathers a variety of information and makes proper use of relevant databases. The FAU detects different types of ML, and predicate offences, generally, in line with the country's risk profile. The cooperation with LEAs and other relevant authorities is smooth. LEAs regularly communicate with the FAU and request their support when investigating proceeds generating crimes. Case studies presented to the assessment team confirm that the FAU and LEAs regularly engage in international cooperation.

173. This notwithstanding, information and criminal complaints submitted by the FAU only to some extent form bases for ML and predicate offences related investigations. The absence of proper feedback by LEAs may hamper the FAU's ability to improve the content and quality of information it provides and respectively prioritise its own course of actions. Further impediments for FAU's effective operation may be the absence of STR prioritisation rules, as well as shortcomings related to the accuracy and currency of information contained in some of the databases. In addition, there are some concerns with regard to STRs processing by some of the reporting entities and the role their SRBs have therein. Strategic analyses are limited to those presented in the NRA and the FAU annual reports and there is a little evidence that they can be used by LEAs to support their operational work. **The Czech Republic has achieved a level of moderate effectiveness in relation to IO6.**

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

174. The conclusions formulated in the course of the analysis below are based on the available statistical data, a number of case examples provided and extensive discussions with the relevant authorities of the Czech Republic.

The authorities of the Czech Republic generally do not refer to "money laundering", but rather to "Legalisation of Proceeds from Crime", an offence under S. 216 of the CC, and to Negligent Legalisation of the Proceeds of crime under s. 217 of the CC. Czech authorities point out that "Participation" (CC Section 214) and Negligent Participation (CC S. 215) are also elements of its law relevant to money laundering, although these are older enactments which closely resemble an offence that might be described more generically as possession of and dealing in stolen property.

175. As already noted under IO6, although the FAU does contribute considerably, most of the ML investigations and prosecutions stem from information gathered by law enforcement agencies either based on complaints from the public, for example in relation to various types of fraud, or their own intelligence, particularly information gained in the course of investigating predicate offences. This conclusion is confirmed by the statistics (please see Table 6 below) which tracks ML matters from the investigation stage through to convictions. Tax authorities also contribute to the initiation of ML cases and, on occasion at least, so do requests for assistance received from foreign authorities.

176. The assessment team was provided with certain statistical data showing that, on average over the years 2012-2016, the FAU criminal complaints (for various offences) exceeded 500 annually (see IO6 and Table 4). Information gathered by the Public Prosecutor's Office (PPO) confirms the very active and positive role of the FAU in terms of filing criminal complaints, intended to initiate criminal proceedings. Of these FAU reports, based on PPO data for the years

2013-15, roughly 200 per year (the numbers vary greatly from year to year) led to the opening of criminal proceedings. However that is where any global statistical data trail ends as FAU initiated criminal proceedings are generally not tracked through to the prosecution and, as the case may be, the conviction stage. Still, it does seem clear that during the last several years, the National Organised Crime Agency or NOCA (particularly its Serious Economic Crime and Corruption Command and the Financial Crime Command together with its predecessor, the Unit Combating Corruption and Financial Crime or UCCFC), made significant use of the reports received from the FAU in the opening stages of the investigation and subsequently.

177. The NOCA, as was the UCCFC, is the police agency most heavily involved in large-scale and complex crime proceeds legalisation (i.e. ML) matters, having a nation-wide reach in matters where damages exceed roughly €6M and fall under the jurisdiction of the High Public Prosecutor's Office. The National Anti-Drug Agency (NADA) also investigates ML as do the Regional Police Directorates (there are 14 Regional Headquarters) and the District Police Directorates (for less serious offences). Investigators work under the oversight and direction of prosecutors whilst the use or application of some special investigative means is subject to judicial approval.

178. The system and structure of the Czech criminal investigation and law enforcement arrangements gives the police the central and most active role in the pre-investigative and investigative stages[25]. Police have at their disposal an extensive array of powers that are used fairly regularly for proceeds-generating offences. While it does appear that a considerable number of reports, suspicions or occurrences of ML result in the opening of a criminal proceeding under CPC s.159, it does not necessarily follow that in all cases LEAs fully exploit the opportunities that are available to actively seek to identify evidence of ML in connection with the investigation of proceeds-generating predicates. Czech authorities advised that this is due in part to the fact that penalties for predicate offence are greater than those for ML.

179. Binding Instruction of the Police President No. 174/2011 "On the Financial Investigation" states that police officers who investigate a crime where property was damaged or where material benefit was gained are to thoroughly investigate and secure the proceeds of crime or equivalent value from the outset. On the subject of joint or cooperative investigations, there were examples of JITs in relation to Europol and bilateral cooperation across borders as well as the use of outside financial experts (accountants, real estate assessors). A number of different specific seizure powers are available (CPC s. 79), including the seizure of property of equivalent value and the FIU's own power to seize temporarily and these are put to use in relation to relevant offences, as is the power to adjourn the prosecution on various bases (CPC s. 159a).

180. The Public Prosecutor's Office (PPO) is divided into various units: 1 Supreme Public Prosecutor's Office, 2 High Public Prosecutor's Offices (Prague, Olomouc), 8 Regional Public Prosecutor's Offices, 86 Public Prosecutor's Offices (including District Public Prosecutor's Office in district of the Capital city of Prague and the Municipal Public Prosecutor's Office in Brno).

181. Czech authorities point out the Section 2(3), of the Criminal Code which introduced the principle of legality stating that whenever evidence of an offence comes to the attention of LEAs, they are duty bound to perform at least an initial investigation in order to "clarify" the matter. This would apply to ML also, but the rule logically reduces the Czech Republic's ability to favour particular offences, such as ML. Therefore in order to prioritise ML Czech authorities created specialised police and prosecution units dealing with financial crime including ML.

[25] CPC Sections 158, 158 a - f.

182. Czech prosecution authorities have recognized over the last several years, the need for national coordination and specialisation. One measure taken in reaction to this was the establishment in 2011, a number of "National Correspondents" (or central coordination points) for various sectors of prosecution activity, including one for ML, currently known as *the National Correspondent for combating financial crime and money laundering, search and draining of proceeds of crime and protection of the financial interests of the EU*. The Public Prosecutor's Office has also set up an Extranet web page through which information is provided to all Czech prosecutors, including information on methodology in relation to ML and case law.

183. As for specialisation of prosecutors, a binding Instruction (no. 4/2009) makes specialization of prosecutors mandatory at the Regional and High Public Prosecutor's Offices and at the Supreme Public Prosecutor's Office, while at the District Public Prosecutor's Offices this specialisation is optional.

184. As a result, among the total of approximately 1250 prosecutors dealing with all offences within the PPO, there are currently 182 specialised ML prosecutors at the various offices as follows:

Public Prosecutor's Office	Supreme Public Prosecutor Office	High Public Prosecutor Offices	Municipal District and Regional Public Prosecutor Offices in Prague	Other District Public Prosecutor Offices	Regional Public Prosecutor Offices
Number of prosecutors specialised in ML	**16**	**43**	**31**	**37**	**55**

CEO Fraud Cases

In 2015, the FAU dealt with several cases of so-called "CEO fraud" (in which the fraudsters use their knowledge, for sending false-billing e-mails, of the identity and business practices of senior managers of the target company). The defrauded companies were usually falsely informed of a change of payment contacts of one of their partners or suppliers. In total in such cases the FAU seized together nearly 270.000.000 CZK (approximately 10.188.679 EUR) and filed criminal complaints. Typically, the predicate was committed abroad, hence the analytical work required substantial cooperation with foreign FIUs and later MLA to return the assets abroad.

Case 1: Company A registered in Saint Vincent opened accounts in the CzR where the managing clerk was an Israel citizen. The FAU received an urgent request from the FIU of Switzerland, about suspected CEO Fraud where Company's account had received a transfer of over 700,000 CHF. The Czech bank detected the criminal activity on its site also and filed an STR simultaneously. After analysing the activity on the Czech account and other documents, the FAU filed a criminal complaint for suspected legalisation (i.e. ML) under Section 216, 217 and likely fraud and seized EUR 352.445. Four supplements followed showing related fund transfers to Hong Kong and then back to the CzR, leading to further seizures bringing the total to € 756.862,- and identifying aggrieved parties in Switzerland and France.

Case 2: This involved aggrieved parties in Belgium and France in a similar scenario involving Company B (limited partnership with unclear ownership structure, established in UK) with a French citizen as the managing clerk of the Czech accounts. After receiving an STR, the FAU contacted the French and Belgian FIUs, leading to a seizure by the FAU of € 463,038 and its filing of a criminal complaint related to Section 216, 217 together with the blocking of a critical transaction in a French bank. The Czech police had been

preparing for a JIT with France, but it now seems more likely that France will take over the Czech portion of the case.

New developments

185. Amendments made in relation to the main ML offences have resolved some of the technical deficiencies that may well have hampered ML investigation and prosecution in certain areas. Notably among these was the creation in 2011 of criminal liability for legal persons.

186. It is noted that the NOCA's Proceeds and Money Laundering Department (a sub-unit of the Section of Serious Economic Crime and Corruption) has been increasing its numbers and now comprises 25 police officers (an increase of 50% since 2014). Czech police more broadly have developed greater capacity in terms of financial investigation. Currently 210 of its members have received some level of training in the area of financial investigation and these officers are spread across the NOCA, as well as Regional and District levels.

187. As the Czech authorities acknowledged in their submissions to the assessment team, certain deficiencies could be found in relation to "clarification[26]" and in the field of financial investigation in the pre-trial stage (and these comments are confirmed by statistical data). Therefore the increase in the number of financially trained investigators is a welcome improvement.

188. Czech Republic has created a Central Register of Bank Accounts with the aim to address delays in obtaining banking information (please see IO6, paragraph 174).

189. In much the same manner, in relation particularly to the abuse of legal persons (corporations mainly) to cloak the flow of assets and the identity of the perpetrators of both predicate offences and ML, the advent of the newly created Register of Beneficial Ownership promises to accelerate the progress of investigations. However, the effects of this innovation cannot truly be appreciated at this point, as the BO register, although it came into being on January 1, 2018, has yet to be usefully populated with a significant quantity of the required data.[27]

190. Both of these new registers will conceivably make a significant difference in the length of proceedings at the pre-trial stage, a difficulty that has no doubt had negative effects on the effectiveness (freshness and availability of the evidence, for example) and, inevitably perhaps, compromised the outcome itself of major investigations. For example, in the course of the NRA Czech authorities examined the work of different investigative authorities with respect to ML in relation to patterns of criminal activity considered to be high-risk areas for the country, including tax fraud, other forms of fraud (including manipulation of a public tender, credit fraud), corruption and embezzlement, mainly. The focus was on investigations in relatively complex matters carried out by the Tax Department, the Department on Serious Economic Crime the Proceeds and Money Laundering, including in a small number of cases, the participation of legal professionals. Among a larger number of cases that these agencies had been investigating within the period 2013-15, 15 cases were considered that had been "concluded" (from the investigators' point of view) by a motion for indictment during the same period. It was noted that the average time spent in pre-trial proceedings was 3.5 years, with the fastest time at 475

[26] This term refers to the initial investigation to determine whether a more fulsome investigation should be performed and a criminal procedure initiated, or whether there is an insufficient basis to continue the investigation.

[27] It is noted that the FAU had been making efforts, before the on-site visit (and following the visit, though this is less relevant) to actively add to and organise the relevant data in these registers and to make the input from the relevant Czech entities easier.

days and the slowest at 3189 days. This seems too long. Prosecution authorities that the assessors met during the on-site visit did express a certain amount of frustration at the length of proceedings under the current CPC.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

191. The NRA, in addition to listing certain patterns of criminal activity as representing a high-risk for ML, also focused in more detail on certain specific situations or phenomena as constituting a high risk for the country with respect to ML. One of these was the observation that the number of convictions for ML was relatively low.

192. Czech authorities did provide the assessors with a modest number of examples of cases in these categories and at various stages of the investigation or prosecution, but relatively few completed cases in these areas. The following is a completed case, referred to for its scale, complexity and results.

'Corruption case'

In a case that attracted significant media attention, the Department of Serious Economic Crime of the Public Prosecutor's Office (PPO), obtained a conviction for ML against a number of individuals with respect to corruption in relation to a public tender that took place in 2008-09. A company known as Promopro had obtained a contract to provide audio-visual equipment and associated services to the Czech government in relation to events to be held in 2009, while the Czech Republic held the Presidency of the EU Council

The case began as a result of the FAU reporting, in January 2011, transfers of 520 million CzK (or about EUR 21 million) involving Promopro, an amount that exceeded that mentioned in the contract. To the FAU, this indicated a possible breach of duties related to another person's property and inefficient spending of the public funds. An Austrian specialised prosecutor for corruption informed Czech authorities about their own investigation and money they had found in Austria and about a UK based company which was a suspect. The FAU, on behalf of Czech authorities, requested that money in Austria be frozen and a MLA request was sent to Austria, concerning 134 million CzK (EUR 5,2 million). In addition, a MLA request was sent to the UK – to interview a witness and to provide relevant information with regard to the company involved in the case. The MLA was executed by the UK in three months. A criminal proceeding was opened in the CzR focusing on whether the Promopro contract had ever been fulfilled. Only a part of the contractual obligation was covered by Promopro, the remainder to be carried out by the subcontractor, who in turn delegated some of the tasks to another subcontractor. All documents relating to these companies were obtained by police, including accounting documents. Bank data was another source of evidence. Experts examined the economic aspects of the case. The subcontractors, some of which were apparently fake or dubious, had no business history, no employees. The prosecution was initiated with 12 people charged, 3 with fraud and ML, 6 for ML only and 3 for Failing to act efficiently (those employed in the Czech government). Nine were convicted for fraud and ML and 3 civil servants were acquitted. The verdict was confirmed by the appellate court after a 6-year trial ending in 2017. As a result assets of a value of 135mil CzK (EUR 5,237,152) will be returned to the government as a damaged party. The total damage is estimated to be approximately 325 million CzK (EUR 12,607,960). The difference between the amount seized and the total damage could not be confiscation, as it had been withdrawn by unknown persons and thereafter disappeared. The flight of the money was in part because the investigation was initiated 2 years after the crime was committed. The assets in Austria have yet to be recovered from Austrian officials.

Convictions and Sentences: 9 individuals convicted, 3 of these for ML and fraud – 2 sentenced to 9 years and one to 7,5 years; 6 convicted for ML received sentences between 3 and 5 years imprisonment. Fines

were imposed up to 100 mil CzK (EUR 3,878,815) and 2 perpetrators were ordered cover the rest of the damage.

193. While the case described above clearly corresponds to ML in relation to offences highlighted in the NRA, the data available for the vast majority of cases where convictions were obtained does not make it possible to establish a clear relationship with such areas. However, the chart below outlines a significant number of investigations (those not based on STRs), prosecutions and convictions obtained for ML (either under s. 216 or 217 CC):

Table 6

ML Investigations by law enforcement carried out independently without prior input from the FAU Investigations by law enforcement (under Section 158 par.3 of the CPC)			**Prosecutions commenced** Prosecution means for the purpose of this statistic cases where the formal resolution on initiation of criminal proceeding was issued.			**Convictions (first instance)** Not monitored			**Convictions (final)** ML = Sections 216, 217 of the Criminal Code 40/2009 Coll. Court Statistical data Sheets		
Cases	**Natural persons**	**Legal persons**	**Cases**	**Natural persons**	**Legal persons**	**Cases**	**Natural persons**	**Legal persons**	**Cases**	**Natural persons**	**Legal persons**
2012											
339	NA	NA	105	103	0	NA	NA	NA	NA	44	0
2013											
369	NA	NA	174	139	3	NA	NA	NA	NA	45	0
2014											
431	NA	NA	296	165	4	NA	NA	NA	NA	73	0
2015											
356	NA	NA	247	172	3	NA	NA	NA	NA	109	0
2016											
381	NA	NA	204	170	4	NA	NA	NA	NA	129	0
30.6.2017											
152	NA	NA	106		14	NA	NA	NA	NA	NA	NA

194. As shown in the table above, since the coming into force (2011-12) the Czech provisions related to criminal liability of legal persons, there have been 28 prosecutions against legal persons (though none has yet resulted in a conviction, however). And while there is an encouraging trend in the number of ML convictions in recent years, there is no indication of what underlying offences are involved. Also, data provided show that a significant number of the investigations, criminal procedures, prosecutions and convictions were related to the less serious offence (or "misdemeanour" as CzR authorities refer to it) of Negligent Legalisation of the Proceeds of Crime under s. 217 of the CC (on average 40% for 2012-15, 48% for 2015, no information for 2016-17 in this respect). As is indicated in the first column, these are investigations that began without initial financial intelligence provided by the FAU as a starting point.

195. It may be that ML based on some of the "target offences" highlighted in the NRA that involve complex structures and financial transactions would be less likely to be revealed by other means than through financial intelligence. These are offences such as corruption, machinations related to public tenders or subsidies fraud. Finally, on an unrelated matter, the assessors do recognise, for the purposes of understanding the data in Table 6, that because cases may well last more than a year, convictions in one year would not necessarily result investigations/prosecutions that began in in the same year.

196. Although there are a good number of convictions in Table 6 above, particularly in the latter years, the clear majority relate to less sophisticated and less complex ML schemes. Many may be, for example, for ML charges that were added to a predicate offence investigation with relatively little financial investigation. However, the assessment team was also advised that the conviction rate in relation to ML prosecutions is roughly 80%, an impressive result in this regard.

197. The assessment team was provided with statistics regarding the number of convictions for proceeds-generating offences (frauds of various kinds, drugs and tax offences), which number in the thousands annually (although a fairly large number were the subject of "summary pre-trial proceedings" indicating that these were less serious offences). When these numbers are contrasted with the number of ML convictions, the result, though not insubstantial, leaves something to be desired. While the Czech Republic does demonstrate effectiveness to some extent a more focussed "follow the money" approach to investigations and prosecution seems to be required.

198. Aside from the statistical overview, a modest number of case examples that did correspond to high risk areas for ML were provided, but only a small percentage were completed cases that would demonstrate that the matter was pursued to its ultimate end, whether resulting in conviction or acquittal. Consequently, based on the information provided, it cannot be concluded that the ML investigations and prosecutions carried out fully correspond to the risk-profile of the Czech Republic.

199. It was noted that Czech authorities do investigate on a regular basis ML cases where the predicate offence was apparently committed abroad. Furthermore, there is some evidence, based on the outgoing requests for MLA and those made by the FAU in relation to ML that Czech authorities do follow up with foreign authorities to seek assistance in relation to ML matters (see IO2) and that this tendency is on the increase. And although the statistical data received by the assessors does not permit a clear overview of whether the ML-related requests pursued deal with the high-risk ML areas identified in the NRA, (as the data do not specify the underlying offence in relation, for example, to MLA requests dealing with ML), there is some evidence to show that fraud and phishing are often the associated predicates. The proportion of foreign refusals of Czech outgoing MLA requests, based on available statistics, appears very small. In addition, there was information from Czech authorities during the on-site about certain difficulties at the investigation stage (especially given the length of this phase of the process, perhaps) in maintaining the motivation to seek and obtain required information from beyond Czech border. Therefore, while the assessors recognize that in certain cases (examples were provided) critical information about the predicate offence was not obtained from abroad and thus the matter could not be prosecuted, it is difficult, based on the data provided, to determine the proportion of ML investigations impacted by such unfruitful attempts to obtain assistance from abroad.

200. As mentioned above, there is a limited ability to favour tackling one type of criminal activity over another. In view of this situation, and while the recent increase in resources and

capacity for some police and prosecution units is a positive development, perhaps there needs to be a further and regular re-evaluation of the appropriate resource levels in order to achieve better results especially in terms of large scale ML investigations, prosecutions and convictions.

Types of ML cases pursued

Stand-Alone, 3rd party, foreign predicate offences

201. A number of cases (at least 27 concrete examples were provided) that were simultaneously "standalone" and foreign predicate ML matters were investigated by Czech police during the last 3-4 years. In some of these, a third party was involved, mostly money-mules. In most cases, the matters had to be adjourned either for a "different execution" (s. 159(1)a), b) of the CPC) or adjourned as indefinite adjournments under CPC 159a(5) (lack of evidence). However some cases did lead to a prosecution and in a smaller number a conviction.

202. Supreme Court judges met on-site confirmed that a conviction for a predicate offence is not a prerequisite to reach a conviction for ML. On the other hand identification of which specific predicate offence has been committed is required. With regard to what exactly is meant by 'identification of the predicate' and what would be sufficient information in this regard if it was committed abroad, the judges stated that at least an investigation would have to have been initiated in the foreign jurisdiction. Czech authorities referred to a potential ML case where a large amount was transferred to a Czech bank by an African country official. The press worldwide identified him as a corrupt politician. Whilst the FAU and other authorities immediately requested further information from the African jurisdiction to pursue the case, no response and thus no reliable information on the predicate was ever received, resulting in the case being abandoned. While this example can be seen as a simple failure of the international cooperation process which was beyond the Czech authorities' control, in the assessment team's view it would be beneficial for the Czech Republic to consider creating an offence which does not require that the specific underlying offence be identified, but merely that evidence be produced to show that the assets were derived from illegal activities.

203. Below are several case examples of different types of ML offences:

International phishing case: In 2011 the FAU filed a criminal complaint regarding wire transfers on account belonging to a company. The managing clerk of this account was the 100% shareholder in the company. Payment in amount of EUR 97.490 from an account in Netherlands was transferred in favour of this company's account. The Dutch bank informed the Czech bank that the payment was fraudulent and the funds likely originated from hackers' attack using the Trojan Horse, and asked for their return. Meanwhile (since the payment arrived before the warning was received) the shareholder had withdrawn a part of the funds in cash and transferred another part in favour of two accounts. After further analysis it was concluded that these accounts were controlled by the same shareholder. The bank, after communicating this to the FAU, blocked the accounts related to the company or to the shareholder. The shareholder was reported, by his family member, to the Police as a potential straw man of several legal persons and in the past two criminal proceedings were launched against him. The FAU seized the amount of EUR 14.415, and submitted a criminal complaint for fraud and legalisation of proceeds of crime (Sections 209, 214 and 216 of the Criminal Code). It was found that the shareholder ("potential straw man") was in fact misused by the other persons. The real straw man set up seven bank accounts for two business companies which served to launder the proceeds acquired from international phishing attacks. Victims of phishing attacks were both natural and legal persons in Netherlands and legal person in Venezuela. The straw man withdrew the money in cash and transferred it to one of the main perpetrators. During the house search the police seized credit cards and passwords for bank accounts, stamps of fictitious companies and forged ID. The case involved intensive police cooperation via Interpol. On the

basis of the criminal complaint the Police succeeded into seizing 2.700.000 CZK (EUR 103.053) and EUR 101.304.

The strawman and other (six) organisers were then convicted. The strawman was sentenced to 3 years of imprisonment.

Metropolitan Credit Union Case: Of the twenty persons who were prosecuted, ten persons were for the predicate crime and for ML, six for money laundering only, as ML was their only role within the conspiracy. The matter was investigated from the beginning in 2010 of the criminal activity up to 2013. The perpetrators, the chairperson and members of the board of a credit union channelled deposits of members of the credit union for the benefit of third-party accomplices and arranged for the assessment of credit worthiness and the approval of the loans to be a strictly pro-forma process, with no preconditions for limiting credit risk. Thus the perpetrators deliberately channelled funds from the credit union to outside entities through fake credits that they approved themselves. The purported credit process was assisted through the use of companies with no history (so-called "ready-made" companies), represented by money mules. The object of business of applicant companies was supported by fictitious, unrealistic business plans. The perpetrators sought to obtain from the Deposit Insurance Fund (part of the GSFT Financial Market Guarantee System), pursuant to Act No. 21/1992 Coll. on banks, compensation for insured deposits including interest up to the amount of compulsory insurance. The perpetrators received an amount of CZK 12 billion (EUR 465,483,512) for the duration of their criminal activity, as each credit union is obliged to insure receivables from deposits according to the Bank Act. In total, the funds seized amounted up to 3.1 billion CZK (approximately 118 million EUR). The amount of approximately 100 million Euros was restituted to victims while the remaining of approximately 18 million Euros was secured in accordance with Section 79a of the CPC and from the accounts of shell companies. Furthermore, properties of these companies were seized. Case is still before the court.

Other case: The Department of Proceeds and Money Laundering, at the time when it processed criminal complaints of the FAU, examined independently cases of legalisation of proceeds of crime, in particular criminal complaints with postponement of fulfilment of customer's order (under s. 20 of Act No. 253/2008 Coll.). It involved an offense of ML under CC s216 (1)a and (2)a or s. 216 (1)a and (4)b para. 1 letter a), par.2 letter a); or Section (a) or Section 216 par.1 letter a) and par.4 letter b) of the CC, or (former) CC s. 252a (1), (3) b or c . 22 cases were initiated in 2012 and 2013. In 13, the matter was adjourned under CPC s. 159a of which 2 were adjourned pursuant to CPC s.159a(5)(lack of evidence). Eight cases were resolved differently, i.e., transferred to a police department with local and material jurisdiction. These cases related in particular to crimes committed abroad where a bank's customer was deceived but promptly reported this fraudulent behaviour to his/her bank in order to block the funds in the account. One case of stand-alone legalisation launched by the Department in 2015 is still under examination.

204. Examples of self-laundering ML investigations were also provided, in relation to theft and drug offences, where convictions had been obtained. While most cases had not yet reached a final verdict, there were a small number of examples provided, however, of convictions in relation to standalone ML where significant sentences were obtained (please see the 'Corruption case' above).

Effectiveness, proportionality and dissuasiveness of sanctions

205. There is some difficulty in assessing Czech results in relation to this issue due to the Czech practice of combining in one the sentences for the predicate(s) with those for ML. It would appear that this is the case, particularly in relation to the offence of "Participation" under s. 214, based on the statistical information provided showing a significant number of matters where the custodial sentence imposed was not suspended. It is noted, however, that in a few case

examples provided, however, even when prosecuted as a standalone and/or 3rd party ML offence for the particular accused, convictions were followed in some cases by substantial sentences, for example in the range of 3 to 5 years (see the "Corruption case" and "International phishing case" above). As pointed out in the TC assessment of R.3, in certain instances, the lesser sentence related to the predicate offence will apply rather than those for CC s. 216-217, but this would only relate to one or two of the 31 required "categories of offences". Therefore there is no significant impact on the effectiveness of sentences for ML.

206. The following table shows the types of sentences imposed over the years 2012-15 in relation to both s. 216 (Legalisation of Proceeds, max. 8 years) and s. 217 (Negligent Legalisation, max. 5 years) of the CC combined:

Table 8: Sentences imposed (2012 – 2015)

§216: Legalisation of proceeds								
Year	**Incarceration**		**Average time of incarceration (months)**	**Community service**	**Prohibition of activity**	**Pecuniary penalty**	**Other penalty including confiscation of property**	**Reference to another authority under Section 222 of the CPC**
	Unsuspended	**Suspended**						
2012	**10**	**11**	**55,1**	**1**	**5**	**1**	**6**	**0**
2013	**6**	**23**	**48**	**0**	**2**	**5**	**4**	**0**
2014	**9**	**31**	**37,8**	**0**	**1**	**6**	**11**	**0**
2015	**8**	**47**	**40,7**	**1**	**4**	**3**	**10**	**0**
§217: Legalisation of proceeds by negligence								
2012	**0**	**17**	**-**	**1**	**0**	**1**	**2**	**0**
2013	**0**	**13**	**-**	**1**	**0**	**0**	**1**	**0**
2014	**0**	**22**	**-**	**3**	**0**	**1**	**1**	**0**
2015	**0**	**45**	**-**	**1**	**2**	**4**	**1**	**0**

207. As can be seen from the Table 8, all convictions under s. 217 for negligent legalisation were followed by suspended sentences and/or some other form of sentencing. For convictions under S. 216 (CC), the sentence is also most often suspended, with a range of about ¼ to ½ of convictions resulting in actual time in custody, which varies from year to year in terms of the average number of months, but ranges roughly between 3 to 4 years (the average in 2012 was slightly more than 4 ½ years, however).

208. Whilst the assessment team is aware that it should not delve too deeply into assessing the adequacy of sentences as between suspended and "unsuspended", particularly when the circumstances of the offence are not known, it is noted that actual time in custody, all other things being equal, logically has a greater deterrent effect. This is likely more often the case when the crime, as is the case for ML, is simply driven by financial gain. This would apply both to the objective of specific deterrence (deterrence of the particular accused convicted) and the broader social objective of general deterrence (deterrence of the public at large and individuals contemplating engaging in ML), particularly since Czech criminal trials are open to the public,

including the media, who may report on the cases. Nevertheless, overall the sentences imposed, as set forth in the Table 8 above, are considered to be adequately proportionate and dissuasive.

Case related to production of narcotics: An accused perpetrator was engaged in the sale of chemical substances intended for a production of methamphetamine, which he tried to mask as part of the operations of a corporation that he controlled. Initially, the Police required information from the tax administration and found that the property situation of perpetrator was not in accordance with legal incomes. Police contact with the FAU further confirmed their suspicions. Following the search of a house and other premises, police seized 10 kg of pseudoephedrine (valued at EUR 68,000), chemical substances worth €188,000, funds and cash for a total value of CZK 6.000.000 (EUR 232,728), EUR 25.000 and other foreign currencies in the amount of CZK 80.000 (EUR 3,102) and bills of exchange of a value of CZK 5.500.000 (EUR 213,320). Police also seized 5 luxury vehicles valued at CZK 5.000.000 (EUR 193,923) and a flat, valued at CZK 1.000.000 (EUR 38,784). The main perpetrator was convicted of production of narcotics and ML and sentenced to 12 years together with the confiscation of assets. The corporation was charged and over 7 million CzK (EUR 271,493), EUR 7,000.00 and 2 Hummer vehicles. The real estate belonging to it was forfeited when the company was dissolved. The accomplice was sentenced to 8 years, in part for trying to create false documents to conceal the ownership of the assets. The ML in this case was only attempted and the sentences for ML are currently under appeal.

Other criminal justice measures

209. Czech authorities advise that when a conviction is not feasible, they can still proceed (where possible and subject to provisions of the S.101 of the CC) to forfeit property. Several examples of when this measure had been applied were presented to the assessment team. This form of confiscation, i.e. non-conviction based confiscation is further elaborated upon under IO.8 as are the other forms of confiscation in criminal proceedings.

210. Although not being a truly criminal justice measure, worth noting is the possibility of confiscating the property acquired from non-taxed income in line with the Tax and Value Added Tax Acts. This measure is also dealt with under IO.8.

211. Czech authorities also refer to matters that are resolved by means of an "Alternative decision", although they have not defined this term, nor given concrete examples.

Conclusions

212. Since the last mutual evaluation, the Czech Republic has improved its technical compliance in a manner that has improved effectiveness (notably through the creation of criminal liability for legal persons). Czech investigative and prosecutorial authorities have improved the results in terms of ML prosecutions. There are now more and more financial investigations being performed by a greater number of investigators with training in this area. During the period under review, the country has also achieved a large number of ML convictions although the clear majority of these relate to less sophisticated and less complex ML schemes. Therefore, work remains to be done by focusing further on the main ML offence, carrying the heavier sentences, and in increasing the number of large-scale investigations and prosecutions directly related to identified high-risk predicates. The length of the proceedings from initial investigation through to prosecution and, as the case may be conviction, has been recognised as too long. Greater attention to streamlining pre-trial procedures in order to achieve a result more promptly is also required. **The Czech Republic has achieved a level of moderate effectiveness in relation to IO7.**

Immediate Outcome 8 (Confiscation)

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

213. Several strategic documents, the latest legislative changes together with the newly available tools and instruments confirm that the confiscation of the proceeds and instrumentalities of crime are given priority in the Czech Republic and that the authorities are committed to applying the principle that "crime must not pay".

214. The Ministry of Interior developed and applied the Strategy to Combat Organised Crime for years for 2011-2014 and 2015-2017. At the time of the on-site visit, the updated Strategy for the years 2018-2023 was in preparation. The Strategy sets several objectives which aim at reinforcing the capacities of LEAs. The emphasis is on financial investigations and recovery of assets: the Strategy's Action Plan foresees further development of the network of financial investigators and improvements in asset management. Special attention is also given to the increased use of the Tax and Value Added Tax Acts' provisions which enable authorities to confiscate (in administrative proceedings) the assets acquired through non-taxed income. In parallel, the Ministry of Justice issued the "Strategy for Development of e-Justice for 2016-2020" which sets up a new case management system for the prosecution service which will enable them to also gather nationwide statistics in the area of seizure and confiscation.

215. In addition, specific operational tools have been developed. For example, the Police introduced the methodological guidelines on how to implement the newly introduced legislation (referred to in paragraphs 253, 256, 257, 258), whilst the Public Prosecutor's Office prepared manuals and guidelines tackling specific matters related to the seizure and confiscation of assets. These documents are accessible via restricted website and are discussed during the training sessions which are regularly delivered. All interlocutors met on-site emphasised their full satisfaction with the inter-agency cooperation with regard to seizure and confiscation. Interviews held on-site, together with case examples handed over to the assessment team and presented in the report, confirm the high quality of inter-agency cooperation in pursuing criminally obtained assets.

216. In 2011, a network of public prosecutors specialised in the seizure of proceeds of crime was established. Members of this network are specialists from the Regional and High Public Prosecutor's Offices and they cooperate under the leadership of the Department of Serious Economic and Financial Crime of the Supreme Public Prosecutor's Office. The authorities advised that these prosecutors also operate as '*the methodology specialists for the internal needs of the Public Prosecutor's Office system*.'

Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

217. The Czech Republic applies confiscation in criminal proceedings. The country also applies a specific form of administrative confiscation based on tax related legislation. "Extended" confiscation in criminal proceedings is in place as of 18 March 2017, but given that this criminal procedure mechanism cannot be used retroactively it has been applied in practice only in some on-going cases in relation to the offences that were committed after its coming into force. Non-conviction based confiscation is also possible based on the new provisions of the CC and, similarly to the extended confiscation, has been applied only to a limited extent.

218. The statistical data from police and prosecutors were presented to the assessment team. It has to be noted that police statistics are the primary source for confiscation related data since statistics provided by the prosecutors concern only confiscation in cases involving money laundering offences. The police data derive from the ETR ("Electronic Case Management

System"), which include all procedural stages in the property confiscation process from initial financial investigations through to the execution of the confiscation order. Nonetheless, it does not include data on mutual legal assistance. The leading financial investigator enters data into the ETR. ETR information is comprehensive and includes the predicate offence, the value and the type of assets seized and subsequently confiscated.

219. The Police informed the assessment team that since 2011, a total value of approximately CZK 8,68 billion (EUR 334 mil.) has been recovered (*this amount covers court decision based recovery as well as assets restituted to the victims in preliminary proceedings pursuant to Art. 80 and 81a of the Code of Criminal Procedure*). The authorities advised that the amount of recovered assets should increase significantly once the on-going complex investigations and subsequent court proceedings, which included significant seizure of assets, are completed. Whilst the value of the confiscated assets appears to be substantial, it is still far inferior to the sums seized and frozen (see Table 9 below). The authorities advised that this gap primarily resulted from the afore-mentioned fact that numerous (and mostly large scale) proceedings were still underway. Given the fact that the pre-trial proceedings last, on average, three and a half years (please see IO7) this reasoning seems adequate as no other impediment in this regard was noted by the assessment team.

Table 9 - seized and confiscated property (2012 – July 2017)

Overview of seized and confiscated property value - all crimes (the Czech Police) (in EUR)					
Year	**Damage[28]**	**Seized property value**	**Rate of damage and seized property value - in %**	**Confiscation orders value**	**Recovered amount (total for period 2012-July 2017)**
2012	1 226 564 885	222 862 595	18,2	22 397 405	334 000 000 €
2013	1 214 503 817	324 847 328	26,7	22 580 823	
2014[29]	916 679 389	297 251 908	32,4	343 453 388	
2015	656 335 878	237 442 748	36,2	45 192 417	
2016	945 610 687	379 389 313	40,1	21 088 960	
2017 (until July)	456 231 462	142 404 580	31,2	8 414 553	

220. In addition, the authorities are convinced that the confiscation figures will also grow due to the recent legislative changes and introduction of extended (in 2017) and NCB confiscation (2015). Nonetheless and as already noted, the assessment team could only partially assess the effectiveness in applying these legal provisions because of their recent entry into force. On the other hand, the on-site meetings confirmed that the authorities were doing their utmost to foster their effective implementation in practice – numerous trainings, practical manuals and guiding instructions are in place to strengthen the institutional capacities in this context.

221. More importantly, the new legislation also obliges the court to reach a decision on all confiscation requests. Prior to these changes, the decision whether or not to issue a decision on confiscation had been discretionary. For example, it was possible for the court not to make any decision on confiscation request thus the property, i.e. the alleged proceeds of crime could have

[28] Damage reflects estimated losses of the state or to a victim. The discrepancy between the 'damage' and 'seized property value' results from the fact that not all losses could be compensated (e.g. if property was destroyed or if perpetrator simply spent the funds obtained through crime and has no assets from which the compensation would be made). S.137 and 138 of the CC.

[29] The amount confiscated in 2014 is significant mostly as a result of a large scale confiscation in so called Metropolitan credit union case (elaborated in IO. 7) where more than EUR 100 million was confiscated and restituted to victims prior to final verdict (please see the case description for further details).

been returned to the perpetrator(s). Czech authorities advised that this situation has happened in practice in two cases. Currently, while the judge may reject the application for confiscation he/she must decide on this issue in all cases.

222. Another legislative reform includes the introduction of explicit provisions according to which the forfeiture and confiscation of an object also affects fruits and revenues deriving from it (Sections 70 and 101 of the CC). Although Czech authorities advised that even before the introduction of these amendments fruits and revenues were subject to confiscation, the revised legislation is expected to expand the attention of LEAs and judiciary on this particular aspect of recovery of proceeds from crime.

223. As it has already been noted, a specific form of administrative confiscation[30] enables authorities to issue an order (so called "hedging order") as a mean to freeze an asset and thus allow recovery of taxes owing, the amount of which has not yet been determined. In practice it functions as follows: if there is reasonable concern by tax administrator that a tax obligation which has not yet expired or a tax that has not yet been established will be irrecoverable at the time of its enforceability, or that there will be a considerable difficulty in recovering the tax, the administration can issue a hedging order.

224. This mechanism allows the tax administration to react quickly and maintain flexibility to the changing market and adapt to new methods used by tax evaders to violate or circumvent their tax obligations. The hedging order enables the Financial Administration to secure both: cash on bank accounts and various assets, goods, inventories, etc. Once tax is assessed, the secured cash on bank accounts and various assets are confiscated. Hedging orders are issued in hundreds to thousands cases a year, mostly for VAT 'carousel' and similar frauds thus confirming the criminal origin of these assets. Key institutions involved in this process, apart from Tax Administration, are police and Customs. Their cooperation on this particular matter is executed within the framework of the so called 'Cobra' cooperation platform. Although the FAU is not a member of this platform, it provides relevant information to Cobra teams whenever requested. An amount of approximately 42,7 million Euros was recovered through this mechanism during the period under review. Given the fact that the NRA considers tax crimes at the very top on the scale of ML predicate offences, this tool seems to be an appropriate response to the threat posed by various forms of tax evasion.

Case "BALKAN"

The Cobra team, within the investigation of the case called "BALKAN", managed to uncover and document a sophisticated structure of mutually cooperating companies, including a well-known domestic corporation and foreign buyers, who factiously traded high-lift trucks. On the basis of reciprocal transactions, these corporations illegally claimed from the local tax authorities an excessive VAT deduction. In this manner, at least 172 million CZK (EUR 6,670,237) were defrauded. The financial administration issued and announced hedging orders in the total value of about CZK 99 million (EUR 3,839,231) where approximately CZK 37 million (EUR 1,434,864) was secured on their bank accounts. Furthermore, motor vehicles and real estate owned by these legal entities were also seized.

225. Police are the main LEA responsible for tracing and identification of criminal assets and instrumentalities. Financial investigators are deployed in different police departments dealing with economic crime, whilst the Special Police Department for Financial Investigations is based in Prague. As already noted under IO.7, 210 financial investigators are deployed all over the country (60 in Prague). As a general principle, they do not take part in the predicate crime

[30] The process is regulated by the Article 167 par.1 of Tax Code No. 280/2009 and Art.103 of Value Added Tax Act No. 235/2004

investigations but only in the parallel financial investigations. This principle, however, has not been evenly applied by different police units.

226. Although there is no specific law which would state that the financial investigations are mandatory in each of proceeds-generated or damage causing crimes, LEAs met on-site advised that in practice they are always carried out in parallel to predicate crime investigations. The *Instruction of the President of the Police No. 174/2011 on Financial Investigations in Criminal Proceedings,* regulates the procedure of financial investigation and seizure of proceeds of crime. Its key feature is that financial investigators shall consistently trace and seize the proceeds of crime or their equivalent value[31] in cases where the predicate crime caused material benefit to the perpetrators or damage to the state, legal of physical person(s). The financial investigation is also conducted for the purpose of executing the pecuniary penalty. The Instruction recognises 2 different forms of financial investigations. The first one concerns serious financial criminality (including ML, tax frauds, organised crime and drugs trafficking) and in these cases the Instruction suggests that investigators create a complete financial profile of the suspects. The other one concerns less serious types of criminality and for this form of financial investigation the approach may vary - it can be the same as for the afore-mentioned serious criminality, or it can be less sophisticated where insignificant damage or material benefits were made.

227. An overview of the most significant types of seizure orders is presented in the table below. The numbers presented confirm the frequency of application of different types of seizure orders against different types of property, which overall proves that pursuing the proceeds of crime is done systematically.

[31] Since the Instruction was adopted in 2011, it did not refer to instrumentalities *per se* given the then definition of criminal proceeds included also the instrumentalities. The understanding of the police is that the Instruction equally refers to instrumentalities even after the revision of the Criminal Code and specific reference to them made therein.

Year	Delivering and seizure of a thing		Seizure of funds in an account at a bank or in other financial institutions, seizure of immobilized securities		Seizure of immovable property		Seizure of other property		Seizure of substitute value		Securing claims of aggrieved persons		Seizure a charged person's property for the purpose of forfeiture of property		Seizure a charged person's property for the purpose of pecuniary punishment (since 1 June 2015)	
	Seized property (in €)	# times this measure was applied	Seized property (in €)	# times this measure was applied	Seized property (in €)	# times this measure was applied	Seized property (in €)	# times this measure was applied	Seized property (in €)	# times this measure was applied	Seized property (in €)	# times this measure was applied	Seized property (in €)	# times this measure was applied	Seized property (in €)	# times this measure was applied
2012	45 154 618	28 087	21 588 412	430	44 365 332	152	16 277 706	24	83 173 420	399	3 158 958	55	1 375 672	35	...	...
2013	54 869 027	41 795	141 299 015	550	40 740 252	188	976 061	124	51 681 637	624	13 429 370	113	8 567 439	15	...	...
2014	75 854 710	39 113	52 056 416	681	48 554 206	149	44 814 813	50	61 631 195	607	958 782	16	5 869 534	13	...	...
2015	32 765 778	35 202	39 148 760	759	58 787 696	152	8 003 057	77	74 709 126	521	7 127 470	117	756 375	22	292 768	9
2016	67 170 199	32 386	101 800 524	862	19 601 928	112	70 442 709	190	84 532 690	534	1 851 822	56	1 489 807	17	7 265 580	106
2017 (until 30 July)	16 287 000	13 785	27 248 960	431	25 352 317	115	13 720 716	43	34 368 223	582	1 306 335	53	944 119	5	4 452 549	60

228. Financial investigators have various instruments at their disposal to collect relevant data on assets. Surveillance, observation and criminal analysis aimed at tracing and identifying criminal assets and instrumentalities is executed through various means such as access to different databases (land, vehicles, the commercial registry, the recently established BO Registry) in addition to other, more common investigative powers such as house search, interrogations, seizure of documents, interception of communications, etc. The access to the Central Register of Bank Accounts is subject to prosecutor's approval. Even though they were granted a direct access to this database, the police advised that they had not experienced any problem in swiftly obtaining bank accounts' data whenever they requested them (the frequency of requests by police to access this database is presented under IO. 6). Police also seek assets hidden abroad, or transferred into investment vehicles (e.g. securities). When seeking assets abroad, police take advantage of national contact points linked to specialised international platforms (mainly via ARO, CARIN and AMON networks) alongside with standard MLA procedures. These channels are used to share information and perform operative checks both in EU jurisdictions and beyond. Such practice enables LEAs to prepare detailed MLA requests focusing mainly on executing seizure orders on property that has been already identified and linked to a perpetrator or a third person based on the aforementioned information exchange. By applying this practice, police manage to avoid unnecessary delays and prevent thwarting the seizure of assets. 'Corruption case' presented under IO7 is an example when the Czech LEAs pursued assets located abroad (please also see the cases below paragraph 273).

229. LEAs do not have their own forensic accountants, but do call upon such experts, whose engagement in relation to LEAs' investigative activities is under a special regime. A national experts list has been created and all forensic accountants listed are at the LEAs disposal.

230. The prosecutor is always informed whenever police initiate investigative activities. Prosecutors may also request police assistance in investigations that they initiated. This is the case mostly when prosecutors (and not police) are the recipients of the criminal complaint. The prosecutor is *dominus litis* of this process and is the only one who can either issue a seizure order (during the investigative phase) or seek a court order once the indictment is in place. Each seizure/freezing order may be challenged. Prosecutors advised that approximately 70% of seizures/freezing orders were not challenged due to the fact that the court has relatively high requirements to grant such orders.

231. The new legislation also enables the prosecutor to request a seizure of a property *'in case the accused person is being prosecuted for a criminal offense, for which imposition of a financial penalty can be reasonably expected due to the nature and seriousness of the crime and circumstances concerning the accused* (s. 347 of the CPC). This specific type of seizure in criminal proceedings aims at securing the execution of a future financial penalty. The Supreme Prosecutors' Office advised that prosecutors undergo specific trainings on how to apply this newly available tool. The use of this measure by the prosecutors significant increased, growing, in total, from 7% to 15%.

KLIMA case

Evasion of Taxes, Fees and Similar Compulsory Payments (section 240 CC)

This case was dealing with reduction of tax duties, when the perpetrators founded and organised a network of companies. The perpetrators created on behalf of companies A, B, C, D and created invoices for simulated advertising services. False invoices were included into accounting of company E as a means to illegally reduce income tax duties of the company. In the course of investigation, the Czech Police (former the Unit Combating Corruption and Financial Crimes) intensively cooperated with the Tax Administration (under Cobra platform) enabling intensive and quick cooperation between police, customs and tax administration with the support provided by the FAU. The Police searched 7 houses and premises of suspected persons and succeeded to seize

CZK 8.000.000 (EUR 310 000) in cash. Furthermore CZK 6.500.000 (EUR 252 076) was seized on bank accounts, 10 vehicles (in the value EUR 213 295) and claims (in the value EUR 387 808) were also part of the seizure. The seizure of funds on bank accounts was possible only because of the parallel financial investigation under Section 8 par.2 of the CPC. Parallel criminal financial investigation initiated by police resulted in obtaining necessary information which was covered by bank secrecy. Close cooperation with the public prosecutor who issued a special type of seizing order was a key for successful freezing of funds.

5 natural persons – among others an attorney and tax advisor – and 1 legal person were accused.

- Damage in relation to state budget was approximately EUR 11.500.000 (CZK 289.000.000)

The court ruled on the imprisonment/confiscation:

Convicted natural person nr. 1 (8 years imprisonment) and EUR 21 000 (substitute value); Convicted natural person nr. 2 (3 years conditionally) and EUR 9 334 (substitute value)

Convicted natural person nr. 3 (5 years imprisonment) and EUR 11 668 (pecuniary penalty)

Convicted natural person nr. 4 (5 years imprisonment) and EUR 10 345 (pecuniary penalty)

Convicted natural person nr. 5 (3 years conditionally) and EUR 9 567 (substitute value and pecuniary penalty)

Convicted person nr. 6 (legal person – cancellation of the person); Confiscation of assets/property: EUR 832 302 in total.

232. One problem identified by LEAs when carrying out financial investigation is the lack of information on predicate offence(s) committed abroad. Although LEAs, as already noted, make good use of different international cooperation platforms, obtaining this information is sometimes slow. Thus in some cases it may not allow LEAs to effectively deal with some types of offences which are committed quickly and the assets put beyond reach shortly thereafter (e.g. phishing).

233. There are no available statistics tracking all the MLA requests (in-coming and out-going) with regard to seizure, freezing, confiscation and asset sharing. Although assessors were informed that the new system of electronic file registry (named ELVIZ) at the Supreme Public Prosecutors has been set up, the compilation and analysis of the data are still underway and will not be available before the end of 2018.

234. Based on the request(s) of foreign jurisdictions, the SPO can undertake coercive and non-coercive investigative measures such as house searches, interviewing witnesses, seizing documentary evidence, providing information on bank accounts and transfers, and also execute freezing and seizure orders. Conversely, the SPO can also request (via letters rogatory) the same measures to be applied by their foreign counterparts. Whilst, in general, prosecutors are satisfied with the responses received from abroad, problems were observed when such requests are sent to some off-shore jurisdictions.

235. With regard to asset sharing, the Czech Republic shares confiscated assets with their EU counterparts. When the value exceeds EUR 10,000 half of the sum is allocated to the Czech Republic budget and the other half to the requesting State. If it is less than EUR 10,000 the amount is considered the revenue of the budget to the Czech Republic. With states which are not members of the European Union, asset sharing is possible if there is a provision in the bilateral or multilateral treaty. The authorities provided anecdotal examples of asset sharing cases with non-EU member states (please see IO.2).

236. The issue of victims' compensation is now given priority over the orders to pay fines or confiscation. Victims can apply for restitution within 60 days after the conviction enters into force. The statistics in the table below confirms this approach:

Table 10 – Victims' Compensation (2012 – July 2017)

Year	Securing claims of injured party(ies)	
	Seized property value	#times this measure was applied
2012	3 158 958	55
2013	13 429 370	113
2014	958 782	16
2015	7 127 470	117
2016	1 851 822	56
2017 (until 30 July)	1 306 335	53

237. There are no limits as to the type and nature of property subject to confiscation. LEAs advised that, for the purposes of execution of confiscation, similar approach is used to secure/seize the proceeds of crime or their equivalent value, and instrumentalities. To confirm the latter, an example was presented to the assessors where, in case of a large scale theft, all instrumentalities used by the perpetrators (PCs, mobile phones, cameras, USBs flash drives, etc.) were seized alongside with the crime proceeds. Police data show that the vast majority of assets seized are funds on bank accounts - CZK 11,9 billion (EUR 458 mil.); real property - CZK 9,5 billion (EUR 365 mil.); securities, bonds, promissory notes – CZK 2 billion (EUR 77 mil.); company shares – CZK 1,2 billion (EUR 46 mil.); 164 vehicles worth CZK 145 mil. (EUR 5,6 mil.); electronics, optics and IT equipment worth CZK 454 mil. (EUR 17,5 mil.). Whilst the breakdown on statistics concerning value based confiscation, confiscation from a third party, confiscation of proceeds which have been moved abroad and confiscation of fruits and revenues deriving from criminal assets are not available, the following case examples confirm that these types of confiscation are applied.

Corruption case of hospital management (relevance for IO8: example of a value based confiscation)

Extensive financial investigation focused on collecting intelligence on the entities of interest. Asset profiling outcomes were used to plan coordinated house searches which primarily targeted the accused fraudsters and resulted in seizing a wide range of assets including not only real estate and vehicles but also luxury electronics, gold bars and antiquities such as vintage stamps, coins and even historical weapons worth some 4.000.000 CZK (approx. 120.000 EUR). Subsequently, the gathered evidence made the investigating authorities extend the confiscation to cover funds in the bank accounts of straw companies and strawmen since the link between those assets and the criminal activities of the fraudsters had been proven. The illicit gain resulting from the criminal activity is estimated to reach some 53.000.000 CZK (approximately 2.120.000 EUR). Despite the fact that the original proceeds had been dissolved and therefore out of reach, investigating authorities, however, succeeded in recovering most of their equivalent value. Based on court decisions, property worth 1.920.000 EUR was confiscated and a pecuniary punishment was also imposed.

Bitcoin case (case already referred under IO6 – relevance for IO8: third-party confiscation)

The fraudster´s spouse, who facilitated the exchange of bitcoins into standard currency via a UK-based exchange office and transferred it to her and her husband´s bank account, was charged with money laundering. The financial investigation resulted in multiple charges against the fraudster, ranging from theft to illicit drug handling. The evidence has clearly shown the origin of 4.000.000 CZK (approx. 170.000 EUR) credited to the bank account of the spouse, allowing it to be considered as laundered criminal assets originating from the predicate crime committed by her husband. From the confiscation perspective, targeted financial investigation resulted in successful seizure of both traced-down digital currency and cash as well as several weapons

amounting to approx. 640.000 EUR, affecting both the fraudster and his spouse. The court ruled on confiscation of all property seized.

Corruption case (case already referred under IO7 - relevance for IO8: seizure/confiscation of property moved abroad)

In the scope of financial investigation, the FAU and police initiated freezing of assets amounting up to 5.000.000 EUR in Austria. The initial freezing was a result of FIU to FIU cooperation and was then followed by a MLA request. The final verdict confirmed by the appellate court in 2017, decided that 5.400.000 EUR were to be returned to the Czech government (as a damaged party). The execution of this confiscation order is still underway.

Coal mining company case (relevance for IO8 – seizure of fruits and revenues deriving from criminal assets)

Through the large scale criminal activity, the accused persons conspired to create a sophisticated fraud scheme. As majority shareholders, fraudsters intended to gain full control over a legal entity (a joint-stock company with the government as its minority shareholder) by purchasing its shares using the legal entity´s own resources. More specifically, the company's assets were tunnelled (i.e. illegally transferred) out of the company to a shell company (registered in a financial centre). Funds obtained in such way were used to purchase the remaining 46 % share interest from the state via fraudster-controlled straw subjects. From 1999 to 2006, the company grew to a leading player within the national energy industry market. With a series of major investments and acquisitions, it widened its influence from fuel extraction sector to heavy machinery and heating distribution and sales. These financial operations have captured the attention of the investigators who identified some controversial aspects clearly linking the transactions with fraudster-controlled network of companies. The financial investigation also focused on revenues gained by the company. Based on asset profiling outcomes some EUR 110 mil. of criminal proceed-based revenues generated over the period 1999 – 2012 became a subject of seizure orders, featuring profits generated from funds stored in numerous bank accounts, gains from purchased shares, securities and other investments as well as real estate property-related profits. The case is currently in the first instance proceedings.

238. There are 2 specialised offices dealing with asset management: Office of the Government Representation in Property Affairs (OGRPA) and the newly created Asset Management Office (AMO) of the Ministry of the Interior. Whilst the OGRPA is a general state agency for property matters and can, *inter alia*, also be in charge of managing property seized during the criminal proceedings, the AMO operates in the latter case only.

239. The AMO has 10 employees, it was established based on the Directive 2014/42/EU and aims at providing adequate management of criminal assets and preventing them from losing their economic value before they are either confiscated or returned to the defendant(s). The Office staff is trained in assets value assessment and their management. Although they have good cooperation with police and prosecutors, it appears that their experience and expertise could be further used if the Office is to take part in the whole procedure of asset recovery, starting from its seizure, continuing with management or sale and then in the execution of the confiscation order.

Confiscation of falsely or undeclared cross-border transactions or currency/BNI

240. The Czech Republic has borders only with EU countries- Germany, Austria, Slovakia and Poland. As it has no external borders with non-EU countries, cash controls are applied only at 5 international airports.

241. For the transportation of cash and bearer negotiable instruments the Czech Republic has introduced a declaration system in line with the EU control system (see R.32 in the TC annex). All

imports and exports of cash or BNIs over EUR 10,000 on entry of the Czech territory from non-EU country must be declared in writing. According to the Act on the Customs Administration (Act No 17/2012 Coll., as amended) in order to check the fulfilment of the obligation, customs have the right to check natural persons, their baggage and their means of transportation, postal and other shipments (Section 35). They also have power to require all the necessary information and documents (Section 58 par. 5). Customs have six sniffing dogs which are trained to detect cash. Assessors were informed that the most common destinations for outbound non-declared cash are either Asian or Post-Soviet countries. However, it would appear that no specific data on the origin of these funds were collected. The authorities have not developed any guideline or risk profile of the cash couriers.

242. According to the section 50 of AML Act (Failure to comply with the obligation to declare cross-border transport of cash) a fine up to 10.000.000 CZK (EUR 387 813) may be imposed.

Number of cases/total amount of fines in the years 2013 - 2017

YEAR	NUMBER OF CASES	WHOLE AMOUNT OF FINES
2013	13	128 000 CzK/ EUR 4,964
2014	27	545 500 CzK/ EUR 20,767
2015	26	219 500 CzK/ EUR 8,512
2016	17	202 000 CzK/ EUR 7,833
2017	18	642 300 CzK/ EUR 24,910

243. Whenever a false declaration is made/undeclared cash is found, customs inform the FAU. If there are indications that cash is related to crime, including ML/FT, customs inform LEAs as well. The Customs advised they the key indicator they use to detect illegal transportation of cash is the origin/destination of cash courier. However no statistical data were provided to the assessment team on suspicious border incidents or on assets restrained due to the illegal transportation of currency and BNI, making it difficult for the assessment team to draw a conclusion on effectiveness of these controls. On the other hand, the NRA makes note of the ML/FT risk posed by transportation of cash and establishes several mitigating measures (please see par.246).

244. The authorities, given that the country is a part of Schengen area, do not perform regular in-land control of cash transportation. In case police, during their controls, come across the cash of unknown origin, it would then need to initiate their investigative actions which target possible ML or FT in order to seize it. Nonetheless, the level of proof required to seize cash for purposes of further investigation is high – reasonable grounds that it derives from criminal activity is required. In other words, police does not have efficient means at their disposal to seize the cash of unknown origin. The NRA discussed this matter and suggested a mitigating measure – introduction of controls and monitoring of intra-communitarian transportation of cash.

Table 11: Cross border transportation of currency and bearer negotiable instruments

Year	Number of declarations			
	Incoming		Outgoing	
	Currency	BNIs	Currency	BNIs
2012	Not available	Not available	Not available	Not available
2013	893	2	544	2
2014	793	1	840	1

2015	786	0	811	0
2016	575	0	1193	0
30.6.2017	294	1	421	0

Consistency of confiscation results with ML/TF risks and national AML/CTF policies and priorities

245. The NRA, prepared in 2016, does not address the issue of confiscation in a comprehensive way. As noted in the previous chapters, the data on confiscation is gathered within the ETR system which is based on the "criminal file" principle. It identifies each predicate crime, but if the criminal file relates to several crimes (such as fraud, forgery and ML) the property seized/confiscated (total amount) is attached to each of these crimes in its total amount. As a result, the table below may contain instances of multiple counting of the same seizures and confiscations in relation to two or more listed offences. It needs to be noted that the overall amounts as presented in Table 9 are not affected by this feature of the ETR system as thereto only total amounts are presented without specific reference to which criminal offence they relate to. Despite this fact, analysis of this data show that the seizure/confiscation is, generally, in line with the National Risk Assessment. The highest values seized and confiscated relate to the following crimes: fraud, corruption and bribery, ML and tax crimes (see Table 12 below).

Table 12 (2012 – July 2017)

Property seized				
#	**Crime**	**Cases**	**Amount (EUR)**	**% of total**
1	Fraud	3341	686 386 200,00	29,22 %
2	Corruption and bribery	243	609 054 500,00	25,93%
3	Money laundering	1061	303 800 500,00	12,93 %
4	Robbery or theft	36 455	252 833 800,00	10, 76 %
5	Tax crimes (related to direct and indirect taxes)[32]	533	218 513 600,00	9,30 %
TOTAL		**41 633**	**2 070 588 600**	**88,14 %**
TOTAL of all crimes		**50 499**	**2 349 139 873,00**	**100%**
Property confiscated				
#	**Crime**	**Cases**	**Amount (EUR)**	**% of total**
1	Robbery or theft	31591	139 240 500,00	33,78 %
2	Fraud	1504	134 247 000,00	32,57 %
3	Money laundering	381	107 220 200,00	26,01 %
4	Tax crimes (related to direct and indirect taxes)[33]	179	6 445 200,00	1,56 %
5	Illicit trafficking in narcotic drugs and psychotropic substances	1413	3 669 350,00	0,89 %
TOTAL		**35 068**	390 822 250,00	**94,81 %**
TOTAL of all crimes		**38 279**	**412 207 170,00**	**100%**

246. The NRA analysed the ML risks deriving from the abuse of intra-communitarian transportation of cash. Another risk area that has been identified is so-called smurfing, an activity where a large cash transaction is divided into several smaller transactions in order to avoid reporting requirements

[32] This figure does not include the funds seized through administrative proceedings.

[33] This figure does not include the funds confiscated through administrative proceedings.

for cross-border transfer of cash. For this reason, the Czech Republic set up a notification obligation for persons importing, exporting, receiving or dispatching EUR 10 000 or more during the period of 12 consecutive months. In practice, an electronic on-line database is updated whenever the customs authority identifies a passenger transferring funds in the amount between EUR 5 000 to EUR 9 999. If this passenger is again inspected during the next 12 months and the overall amount exceeds EUR 10 000, then he/she would be in violation of the notification obligation subject to administrative proceedings.

247. The NRA did not elaborate on types of predicate offences corresponding to cash smuggling, whilst the authorities consider tax crimes, drug trafficking, fraud and corruption as the most common criminality preceding cash smuggling.

Conclusions

248. Since the last evaluation the Czech Republic has updated and improved its legal and institutional framework for confiscation of proceeds from crime. Search, seizure and confiscation of criminal assets are given priority by the policy makers. Relevant institutions are properly equipped to trace assets and instrumentalities of crimes whilst parallel financial investigations are regularly carried out and the amounts seized and confiscated are significant. However, as some of the reforms (e.g. the introduction of 'extended confiscation') have been completed and brought into force only since early 2017, the authorities were not in a position to demonstrate the effectiveness in their application in practice.

249. Notwithstanding the significant value of assets confiscated so far, the gap between the assets seized and those confiscated remains substantial, this being a consequence of excessively long proceedings in complex economic crime cases.

250. The Czech Republic diligently applies the requirements of the relevant international treaties, seeks assets abroad and executes foreign seizure, freezing and confiscation orders. The country implements the EU legal framework on cross-border transportation of cash/BNI, but the effectiveness in this area needs further improvements. The statistics and case studies presented confirm that the confiscation results reflect the risks elaborated in the NRA. **Overall, the Czech Republic has achieved a substantial level of effectiveness for Immediate Outcome 8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9 (FT investigation and prosecution)

- During the final stages of the preparation of the NRA and since that time, a certain number of cases have been brought to light that confirm the realistic possibility of FT activities in the Czech Republic. The authorities have reacted to these new incidents by undertaking several investigations related to foreign terrorist fighters and other terrorism and FT related occurrences. One of these cases has reached the prosecution stage and the relevant authorities have paid appropriate attention to the relevant developments and have instituted programmes intended to mitigate these threats.

- Financial investigations are carried out in all terrorism related investigations. In some cases LEAs have managed to plausibly identify the respective roles of the suspects in the FT related scheme. In one case a would-be foreign terrorist fighter was intercepted while on route to join a terrorist group in an important conflict zone.

- Concerns about FT appear to be a part of the general CzR anti-terrorism strategy as set forth in the NSA.

- One prosecution which was not technically for FT (because the investigation originated based on foreign intelligence rather than evidence that would be admissible in court proceedings), resulted in a number of convictions and significant sentences. This demonstrated effective disruption of organised terrorism-FT activity and leading the assessors to conclude that a "true" FT case would be dealt with in an effective and dissuasive manner.

Immediate Outcome 10 (FT preventive measures and financial sanctions).

- As a member of the EU, the CzR is negatively impacted by the shortcomings identified in the EU legislation resulting in delays of implementation of targeted financial sanctions pursuant to UNSCRs 1267/1989 and 1998. The Czech Republic has introduced a national mechanism to remedy these deficiencies. This mechanism, although not requiring immediate freezing of assets but submission of a STR by a reporting entity, still ensures some elements of an effective system. Shortcomings are identified with respect to communicating the designations at a national level.

- The Czech Republic has no domestic mechanisms apart from ones developed under the EU framework for implementation of the UNSCR 1373 to directly cooperate with foreign jurisdictions to give effect to action under the freezing mechanisms. The country initiated no listing/de listing requests during the period under review. There were no written guidelines for designation and de-listing procedures in force at the time of the onsite.

- Apart from larger financial institutions, there is no clear understanding among obliged entities on their freezing obligations. The latter consider that where there is a match their only obligation is to contact the FAU for further instructions. Little is being done to detect funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities. Nevertheless, there have been some false-positive matches identified, which demonstrates a positive practice.

- Technical deficiencies related to the freezing of funds and other assets of terrorist-related persons without delay, definition of funds to be frozen, as well as deficiencies identified with regard

to timeliness of STR reporting and the role of SRBs in the reporting process have a negative impact on the effectiveness of the system in place.

- The NRA assessment of the risk of NPOs' exposure to FT as high. The assessment was based only on some hypothetical examples of FT abuse. As a result, the Czech Republic has not identified the subset of NPOs actually falling under the FATF definition. The results of the NRA were disseminated to the supervisory authorities and the REs, while they have not been sufficiently discussed with the NPOs. The latter appeared to be unaware of the CFT measures in place and potential ways of NPO's misuse.

- Measures taken by the authorities with respect to prevention of terrorism related persons and entities from raising, moving and using funds and abusing the NPO sector, are consistent with the Czech Republic FT risk profile only to some extent.

- The Czech Republic has not established risk-based approach towards the NPO sector. Although several authorities are in charge of supervision on NPOs' activities at different stages, there is no targeted risk-based supervision or monitoring of the sector.

- Limited outreach is provided to the REs and NPOs on their FT related obligations.

Immediate Outcome 11 (PF financial sanctions)

- Implementation of the UN TFS on PF is not ensured "without delay". The measures in place are identical to those applied in relation to the UN TFS on FT, displaying some elements of an effective system. There are some shortcomings with respect to the freezing of funds and other assets of proliferation-related persons, the definition of funds to be frozen, as well as deficiencies with regard to the STR process.

- In one case, the authorities demonstrated effective co-operation and co-ordination leading to identification and freezing of assets of the entity which had links with the designated entity. Consequently, the Czech authorities initiated a procedure for designation of that entity, which resulted in inclusion of this entity in the sanctions list pursuant to the UNSC Resolution 1718.

- There is an uneven level of understanding of PF-related TFS obligations among different obliged entities. Larger financial institutions rely on commercial databases to identify matches with sanctions lists. It appears that little is done to detect funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities. Other REs have almost no knowledge on PF TFS and their obligations in this respect.

- Supervision on implementation of TFS forms a part of each inspection conducted in relation to financial institutions. However, sanctions are not applied in a proportionate manner. Limited training on implementation of TFS has been provided to the reporting entities. Although the CNB developed a guidance on procedures for implementation of the UNSCRs by the financial institutions, the representatives of these institutions met on-site were not aware of this guidance. No guidance was developed for other types of obliged entities.

Recommended Actions

IO.9:

- CzR intelligence services, the FAU and police authorities should ensure that they stay in step with the changing landscape in relation to FT by, inter alia, maintaining close contacts with foreign counterparts;

- Relevant CzR authorities should in all significant investigations quickly and aggressively follow the financing trail in parallel with investigations related to terrorism offences from the outset;

- The CzR should clearly establish, express and, as appropriate, continually re-evaluate the risk level for FT activities and inform reporting entities accordingly;

- CzR authorities should ensure that they maintain work on prevention, disruption, de-radicalisation in the relevant communities, particularly with respect to FTFs.

- The authorities should monitor the court proceedings concerning FT offence, including penalties applied to FT convictions and consider whether they are sufficiently proportionate and dissuasive.

FT preventive measures and financial sanctions (IO10) and PF financial sanctions (IO 11)

The CzR authorities should:

- Ensure implementation of UN TFS on FT and PF without delay enabling a prompt application of freezing measures for the duration of the validity of an action initiated by the UNSCRs, to the comprehensive scope of the property subject to suspension.

- Take further steps to ensure that the FAU communicates the designations and further amendments in the UN TFS on FT and PF to obliged entities, and the later promptly update their databases accordingly.

- Develop a country-specific guidance of implementation of the UN TFS on FT and PF for reporting entities, and provide regular trainings, with the emphasis on DNFBPs sector.

- Establish a domestic legislative framework with respect to implementation of targeted financial sanctions pursuant to UNSCR 1373.

- Revise or conduct a new in-depth risk assessment of the NPO sector to identify ones that are at risk of the FT abuse. Adopt a targeted, coordinated, RBA to oversight of higher risk NPOs, including outreach to and awareness raising for NPOs and the donor community, with a focus on end use of NPO funds. Provide further regular trainings on possible misuse of the NPO sector for FT purposes to the NPO sector.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

251. There is a degree of uncertainty about how to state in a single word the level of FT risk within the Czech Republic, given the manner in which the conclusions are formulated in the NRA (discussed in detail under IO1). However, based on discussions with the Czech authorities, on all of the information related to FT contained in the NRA and, to a lesser extent, in the NSA, it can safely be concluded that the authorities understand the risk level for FT to be, at its highest, "moderate".

252. As for the prosecution of FT activities, at the time of the on-site visit one case was in the prosecution phase. The case does not demonstrate FT in the usual or classic sense of providing money or valuable resources to persons involved in terrorism. However, under the broad definition of the FATF it may be considered to be a FT prosecution in the broader sense of support and encouragement of terrorist activity. Details of the case are provided below. So far there has been no conviction for FT in the Czech Republic.

Case 1. In this case, where a prosecution was underway at the time of the on-site, 3 suspects are involved in the context of ISIL-related allegations. A local imam at the time living in the Czech Republic is alleged to have encouraged and arranged the trip of 2 people who travelled to fight for or assist ISIL in the relevant conflict zone. At the time when the investigation began, the investigation involved 4 suspects and the imam was

suspected of having provided financial support to 2 persons, but there was no sufficient evidence to support this accusation. Currently, the prosecution against 3 of the 4 suspects is being conducted on the basis of the newly introduced CC s. 312e ('Support and Promotion of Terrorism')[34]. All 3 are being prosecuted in absentia since they are all located outside the Czech Republic.

253. Other cases where FT investigations were concluded include those where investigations were either suspended or further pursued under different terrorism-related offences. Both scenarios were the result of lack of admissible evidence on FT. The cases mostly concern support or attempts to provide support to foreign terrorist fighters, terrorist organisations or groups. Further details of these cases (as far as they were made available to the assessment team) are provided below.

254. At the time of the on-site visit, the NOCA was dealing with 10 investigations in progress (though one was suspended because of information suggesting that the suspect had died), of which the majority were based on non-religious terrorism sympathies in relation to a conflict zone. CzR authorities reiterated that in such cases, the FT aspects were investigated. It should be noted that these investigations were initiated before the coming into force of the new FT provision, which shows that conduct of this kind was taken seriously and pursued effectively throughout the period under review.

255. Aside from the investigations referred to above, the following case involves FT allegations that were investigated by Czech authorities.

Case 2. The investigation concerned a plan by several individuals to obtain weapons for a foreign terrorist organisation. In this case, a request to supply arms and munitions was identified and started to be observed by a foreign partner law enforcement agency, raising suspicion that the weapons were destined to a foreign terrorist group. Later on, a suspect was identified. As the subject proved to have a certain connection with the foreign country which had identified the initial threat, a MLA request from the CzR to this jurisdiction followed. However, local authorities explained that they could not provide the requested information on the basis that it would interfere with their own investigations. As a result, the Czech law enforcement authorities had to temporarily suspend the case pursuant to the Section 159a Subsection 5 of the CPC as all requirements for charging an individual with the crime in question had not been met. However, should the reasons for the case suspension cease to apply, the assessment team was assured that the case can and will be reactivated, i.e. criminal proceedings on the matter would be reactivated. No further details on the matter can be provided at the moment due to security and confidentiality concerns.

256. Given that a number of terrorist/FT cases are being or have been investigated and one being prosecuted (that touches upon the FT risk related to Islamic radicalism and to FTF), there is evidence that the country's efforts are in line with the country's FT profile. In addition to the concrete results in terms of investigations and prosecutions, the actions taken by the Czech Republic in the wider sense to increase their level of preparedness and capacity to deal with investigations and prosecutions relating to FT also deserve to be noted.

Legal, structural and institutional responses to terrorism and TF risks

257. First, the amended FT provisions (principally new s.312d) are viewed as largely in line with the FATF standards. In terms of investigations and prosecutions related to IO9 generally, the Czech authorities, though they have limited ability to give priority to particular types of criminal investigations (S. 2(3) of the CPC) have equipped themselves with specialised terrorism and FT units, all of which have received and continue to receive training in relation to terrorism and FT.

[34] After the on-site visit and based on additional evidence gathered, TF charges were added in the prosecution against imam and two other persons.

258. Since 2011 the Public Prosecutor's Office (PPO) system includes a position of National Correspondent (or coordination point) for terrorism, extremism, extraordinary events, protection of cultural assets and crimes against the environment. Based on subsequent amendments of the relevant directive[35], the National Correspondent is now responsible for "combating terrorism, extremism and hate crimes".

259. The PPO has also created an "Extranet" (or internal data base) that is accessible to all Czech prosecutors and contains, *inter alia*, information about methodologies and case law in the areas of concentration of the National Correspondents. Some information is available to prosecutors about FT, but more confidential information is only available to prosecutors specialised in this area, the number and distribution of which is set forth in the table below:

Public Prosecutor's Office	**Number of public prosecutors specialised on FT**
Supreme Public Prosecutor´s Office	2
High Public Prosecutor´s Offices	6 (4 in Prague, 2 in Olomouc)
Regional and Municipal Public Prosecutor´s Offices	16 (usually 2 on each of them)

260. The area of FT is given special attention in the Public Prosecutor's Office system, which is documented also by introducing the so-called "information obligation" vis-à-vis the Supreme Public Prosecutor's Office[36]. All public prosecutors are thereby obliged to notify the Supreme Public Prosecutor's Office of any new case related to terrorism or aimed against the foundations or security of the Czech Republic, foreign state or international organisation.

261. The Czech prosecution authorities with whom the assessors met provided descriptions of the training programs that prosecutors and judges have received over the last several years. These included one or two-day sessions where foreign authorities with more hands-on experience with terrorist attacks and terrorist activity and behaviour within their borders engaged CzR authorities in discussions about the use of covert investigation techniques, the use of intelligence in criminal proceedings and other related topics. In other training events and written material distributed to the specialised prosecutors (chosen on the basis of their experience in dealing with financial crime, organised criminal groups and other related matters) issues are dealt with such as typologies of terrorism and FT, the reaction and role of prosecutors in relation to a potential terrorist attack and other matters.

262. The prosecutors confirmed that the FT offence, as amended, is now broader and clearer. The FT offence falls under the group of criminal offences where all special investigative means are applicable. Even though this had been the case even before the FT offence was amended, these investigative means are more frequently applied since the broadening amendments entered into force. Specialisation was then introduced and information exchange facilitated.

263. The Czech Republic has 3 intelligence services – the Security Information Service, the Office for Foreign Relations and Information and Military Intelligence. Intelligence services are engaged in detecting and uncovering networks of terrorist organisations, radical-minded and armed groups and

[35] Provision of the Supreme Public Prosecutor no. 2/2013, on National Correspondents and their expert teams, as amended (2016); this Provision also follows up on Section 25 of the Act no. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, as amended.
[36] This obligation is stipulated in Article 1 (1) item 6 of the Instruction of General Nature of the Supreme Public Prosecutor no. 10/2011, on Information, as amended.

their supporters with emphasis on financing their illegal activities. The role of intelligence services in the area of FT is mostly ensuring the gathering relevant information and sharing such information with relevant authorities.

264. The intelligence services are cooperating with each other and use, for these purposes, a specialised classified communication channel.

265. Furthermore, the intelligence services which are working on the operative level can exchange relevant information with their foreign counterparts. Most effectively such exchanges are realised on a bilateral level, although cooperation on the multi-agency level is not excluded. For this latter purpose, THE Czech intelligence services are members of several formal and informal platforms dealing, *inter alia*, with the issue of financing of terrorism.

266. On the national level the intelligence services cooperate with the National Organised Crime Agency of the Police (NOCA), Financial Analytical Office (FAU), General Financial Directorate (GFD) and other relevant state authorities as appropriate. The intelligence services can share all relevant information regarding terrorism and its financing with the NOCA most effectively within the regular meetings of the National Contact Point against Terrorism (NCPT). The NCPT has been established as a permanent working operational platform composed of specialised police officers and representatives of intelligence services. It meets on a quarterly basis and *ad hoc* meetings are called when they are needed. For example important events outside the Czech Republic would prompt such *ad hoc* meetings (e.g., the attacks in Nice, Paris, Brussels). The NCPT provides a platform for the sharing of intelligence information quickly, provided such sharing would not have a negative effect on future intelligence interests. Both the NOCA's own operational information and that provided by foreign intelligence agencies may be used as the basis to initiate a Czech investigation, unless the foreign intelligence service states otherwise.

267. NOCA obtains information from the banks and public communication network providers in order to prevent and detect threats in the field of terrorism. This power is not dependent on the initiation of criminal proceedings and has been put to use in recent years. In addition, police and prosecutors have a number of powers at their disposal (see the analysis of under R. 31 in the TC Annex), including covert means such as covert searches, controlled delivery, and the interception of communications. NOCA members interviewed on-site confirmed that they make use of these powers, but that they could not comment, understandably, on the use of particular investigative techniques in relation to identified cases.

268. The FAU also cooperates with the intelligence services in the area of financial analysis in cases of serious suspicion of FT and such cooperation takes place regularly.

TF identification and investigation

269. From 2015 the Police dealt with about 40 suspicions of FT yearly. Most of the suspicions arise initially directly as a result of police work (about 30 cases), the remainder coming from information disclosed by the FAU. As already noted, at the time of the on-site visit, NOCA was dealing with 10 investigations in progress. State of play and particular details of these on-going investigations could not be shared with the assessment team for confidentiality reasons.

270. FT is always a mandatory part of the investigation of each criminal case associated with terrorist criminal acts. In practice, investigation of a terrorism related offence includes financial investigation with detailed analysis of bank accounts and transfer to or from the suspects (their financial 'activity'). Investigators also prepare a 'financial profile' of the suspects. These findings are ten used to identify/create a link to any potential financer.

271. Both the NOCA and the FAU exchange information with the intelligence services and in the case of the NOCA, this is done on a more formally established basis via the NCPT. The suspicions are often related to radical Islamism. Most cases never reached the prosecution stage but were closed once the investigation failed to discover sufficient evidence to demonstrate that the relevant criminal offence was in fact committed. The interviews held onsite confirmed that the FAU and NOCA officers are equipped with knowledge and means to identify potential FT activity. The FAU has two analysts specialised in identifying potential FT. These are former police and intelligence officers who dealt with such matters in their previous capacity. They also receive, in addition to regular training, specialised training related to FT detection. NOCA officers have joint training events (conducted by both domestic and international experts) with the FAU analysts on terrorism and FT matters.

272. The FAU receives the information about potential suspicion of FT via STRs. Such cases are always prioritised and processed thoroughly and carefully, checking all relevant databases and also discussing the matters with the coordinator of international sanctions. Further, the FAU then discusses its findings with LEAs in face-to-face meetings. The FAU as well closely cooperates with intelligence services on detection and assessing the relevance of given suspicions. The FAU can provide information to the intelligence services and can also obtain information from them. The FAU in fact does make use of these possibilities frequently. As noted under IO6, the FAU also received information on the FT suspicion from reporting entities and foreign counterparts. These were related to partial matches with designated persons under the TFS regime. Information on the FT suspicions received from the foreign authorities mostly concerned flash reports that countries disseminate to foreign jurisdictions requesting information on persons designated in their national lists. Although the FAU disseminations did not lead to an investigation on FT, the example provided below presents the way the FT related suspicious transactions are analysed.

Description of a FAU analysis case: The FAU provided the Police with information about a natural person living in the Czech Republic and actively participating in an Islamic foundation based in therein. This person had several accounts in various currencies (CZK, EUR, USD and CHF). Rights of disposal for these accounts were shared with two other natural persons from the same Islamic foundation. The FAU received information about an outgoing transaction in the total amount of EUR 7.100 in favour of an account in Albania. This transaction had not been realised and the bank suspended and reported the attempt because of suspicion of possible FT.

The natural person ordering the payment provided only some information to explain the transaction, but this information was not considered satisfactory by the FAU, which reported the transaction and the circumstances to the Police. Beyond information described above the FAU within its expertise in intelligence detected all accounts belonging to that natural person, managing clerks authorised to conduct operations on these accounts, their potential linkage with the Islamic foundation, contact information for these persons and their accounts. This information was then provided to the Police with a special note highlighting its potential added value for unit dealing with FT. Further actions, which included intensive cooperation between the FAU and police, confirmed that the purpose of the transaction was legitimate and had no links with potential FT.

273. The Czech authorities point out that on the basis of one case which had been active at the time of the NRA**,** they provided guidance to the obliged entities in relation to FT, consisting in part of methodologies observed in foreign countries that have had more experience in this respect. Based on this analysis, the FAU discussed possible risk factors and suspicious indicators (or “red flags”) with the reporting entities, although these indicators had not yet been formally adopted and disseminated to the reporting entities by the time of the onsite visit. Mitigating measures were also summarised in the NRA and distributed to relevant entities.

274. As of August 2016, the supervision of terrorist criminal offences is performed solely by public prosecutors of the High Public Prosecutor's Offices (Prague and Olomouc). For practical purposes, virtually all cases are supervised by the Prague Office.

TF investigation integrated with and supportive of national strategies

275. The NSA produced an Action Plan which was to begin implementation in 2017. As opposed to the NSA, the Action Plan is not public and the assessors were not provided with this document because of its sensitive content. From the interviews held on-site it appears that risks involving money-exchange services and cash couriers were referred to in it. However, it is not clear what threat level was assigned to these areas and the assessors were referred to no investigations focusing on such operations. The NSA included a recommendation that a provision be made under Czech law for the use of intelligence as evidence in particular with regard to terrorism and FT related cases. Based on a much earlier criminal matter (from 2008) in which the PPO sought to justify its use of military intelligence as a basis for a criminal proceedings, the Constitutional Court rejected the PPOs position, but did state that if the state was directly threatened (as in a terrorism case), it would not foreclose the possibility of the PPO legally using such information for these purposes. Although there has not yet been any legislative amendment in this regard, preparatory work is underway within the inter-institutional working group coordinated by the Ministry of Justice. This must be looked upon as a positive and welcome development, though it bears reminding that the ability to use intelligence as evidence in Court proceedings is beyond the requirements of the FATF standards.

276. The NRA, whose Action Plan can be considered as a strategy in this context, provides some rather general measures to strengthen investigation and prosecution of FT. The NRA analysed a case of FT investigation which helped identify new risk factors and creating "red flags" for the reporting entities. The assessors were provided with the summary of these red flags, which seem reasonable. However, it was not considered appropriate or necessary to list these red flags in this report. The Action Plan also includes some measures targeting NPOs and their vulnerabilities to FT.

277. Another strategic document was prepared in 2013 by the Ministry of the Interior (Strategy for the Fight against Terrorism) which resulted in the development of the "Action Plan for the Fight against Terrorism" for the years 2016 – 2018. The Action Plan consists of three independent prongs: legislative proposals, an "Anti-terrorism Package" (classified) and a proposal on increased security at international airports in the Czech Republic. All of these have elements that apply to FT. For example, one of the legislative proposals deals with measures to enhance inspections of trans-border cash transfers. It is, however, not clear to what extent this 3-prong action plan had been implemented by the end of the on-site visit, however.

278. Overall, on the basis of extensive discussions with Czech authorities, it can be concluded that FT investigations and the associated financial investigations are integrated with all significant counter-terrorism investigations. As to the link with broader national counter-terrorism strategies, the absence a unified approach in establishing clear strategic lines prevents assessors from concluding that this core issue was achieved to significant extent.

Effectiveness, proportionality and dissuasiveness of sanctions

279. Since there have not yet been any convictions for FT *per se*, there are no examples as yet of the application of sentences provided under s. 312d, the newly-created FT offence (nor under s. 312e – 'Support and promotion terrorism'). However, there is an example of dissuasive sentencing in relation to offences charged and prosecuted amidst allegations of FT, but where admissible evidence of FT could not be produced to a Court (see under alternative measures below). In the assessment

team's view, the multiple convictions and firm sentences handed down in this case leads to a reasonable assumption that cases prosecuted under the new FT legislation would also be punished, in the case of a conviction, by equally dissuasive and proportionate sentences.

Alternative measures used where TF conviction is not possible (e.g. disruption)

Case 3: In the Czech Republic and two other countries, a group of people was involved in the procurement of funds, the acquisition of false personal and travel documents and the recruitment of fighters for an organisation, which aimed to create a state entity in a form of an emirate or a caliphate. Investigation began on charges of aiding and abetting a terrorist organisation (under CC s. 311 and 24(1)c) since the current FT provisions of the Czech Criminal Code had not yet come into force. Ultimately, however, no admissible evidence of the FT side of the offences could be produced before a court since information to this effect, though credible, had been obtained in the form of intelligence provided by the German secret service. After a thorough investigation, involving a financial investigation and other investigative measures (such as house searches), a prosecution was initiated in relation to the underlying criminal offences (including participation in an organised criminal group, forgery of personal documents, counterfeiting currency, weapons and drugs charges, obstruction of justice) and convictions were obtained in 2013. Of the 9 individuals convicted, all received prison sentences ranging from 3 years to 6½ years. In addition, a confiscation order was issued in relation to one of the convicts, while others (non-CzR citizens) were deported based on their involvement in serious criminality.

280. The above-noted case provides evidence of the CzR authorities' commitment to investigating, prosecuting and where convictions are obtained, punishing by dissuasive sanctions individuals involved in providing financial and material support to a terrorist organisation, even though the suspects could not technically be convicted of FT because of the circumstances. This case also provides an example of the use by the NOCA of foreign intelligence and appropriate investigative techniques in relation to what appeared to amount to FT, even though it could not be proven as such in a court.

281. In another matter a successful disruption of terrorism was based on prompt action by Czech authorities, which averted the participation of the person involved in terrorist activity in support of ISIL and resulted in his conviction. Although a financial investigation was carried out, the convict appeared to have been self-financed. In 2016, a would-be FTF was intercepted in Turkey en route to join ISIS as a combatant. The 25-year old man, a Czech citizen who had apparently been "self-radicalised" and had no affiliation to the Muslim faith, was returned to the Czech Republic, prosecuted and convicted. Although his sentence had initially been lower, it was increased to 6 years' imprisonment on appeal. This incident appears to have raised the level of awareness and concern among the relevant Czech authorities in relation to the threat of FTFs from within the Czech Republic and their financing.

282. In terms of prevention or general disruption of terrorism and FT, the SAIRO (System for Analytic Identification of Radicalised Inmates) programme of the Czech Prison authorities deserves mention. The project, created by a Czech Ph.D. student for the Police Academy, seeks to assist authorities in detecting manifestations of radicalisation during imprisonment. It is based on collecting information gathered via international cooperation and the analysis of these data. The programme is intended, at least in part, as a mean to educate prison staff and examines case studies in sessions held for their benefit.

283. The Czech authorities also collaborate in other educational and awareness raising activities with foreign counterpart. For example, the FAU hosted a workshop in September 2016, with participation from a number of European countries that have a history of FT occurrences.

Conclusions

284. Czech police and prosecution authorities appear to be aware of the risks their country faces and have taken actions, in terms of institutional organisation, specialisation and training. Given the moderate FT risks that have been found in the geographic and general context of the CzR, the efforts deployed by CzR are considered as adequate. FT is always a mandatory part of the investigation of each criminal case associated with terrorist criminal acts. At the operational level, the authorities have reacted to their risks by opening a number of FT investigations. They launched one prosecution which is currently underway. Another investigation and prosecution for providing material and financial support to a terrorist organisation in circumstances, where FT was suspected but could not be proven by means of admissible evidence, did nonetheless produce convictions and yield substantial sentences.

285. FT investigations are integrated with national counter-terrorism strategies, although establishing the appropriate linkages is hampered by the absence of a clear unified strategy in this regard. In addition, the Czech authorities should sustain their commitment to preparing for, detecting and providing an intensified operational response to FT risks in light of an ever-evolving landscape with respect to terrorism and FT. **The Czech Republic has achieved a substantial level of effectiveness regarding IO9**.

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

286. The Czech Republic, as an EU member state, applies EU legislation when enforcing TFS. Consequently, certain shortcomings identified in this matter, namely delays in transposition of UN designations into the EU legal framework[37], affect the Czech Republic ability to effectively implement relevant UNSCRs without delay. Notwithstanding the recent reduction of delays between the date of designation by the UN and its transposition into the EU framework, concerns remain with regard to timely implementation of the UN TFS. These issues are further analysed in the TC annex (see Recommendation 6).

287. In order to overcome the time gap between the publication of new designations by the UN and their transposition into the EU framework, the FAU introduced Methodological Instruction 5 (MI5). This methodological instruction concerns all reporting entities. In particular, when the new designation is made by the UNSC, the FAU circulates this information immediately to the reporting entities. MI5 provides that the reporting entities, whenever they come across a transaction involving person or entity designated under the UN TFS (before transposition into the EU List), they shall consider it as a suspicious transaction and submit a STR. While the assessment team acknowledges this positive step taken by the CzR authorities, the concern still remains whether this measure does indeed ensure implementation of sanctions without delay. As a matter of fact, the requirement as established in MI5 does require the reporting entities to consider the lists as a 'red flag' i.e. as an indication of FT which requires submission of STR. The authorities indicated that the funds would be further suspended by virtue of application of the AML/CTF Act (Article 20), i.e. the obliged entities would not proceed with the transaction within 24 hours after submission of the STR, waiting for the FAU decision of suspension of transaction or seizure of assets. While this domestic mechanism does not set a direct obligation to freeze the assets of designated persons and entities for duration of the

[37] The EU sanctions database includes UN designations which are not yet implemented via EU regulation (with a specific indication of them being pending).

validity of an action initiated by the UNSCRs, application of the AML/CTF Act may, to some extent, prevent terrorists from raising, moving and using funds.

288. The process of making proposal for designation to the respective UNSC Committees under the UNSCRs 1267/1989 and 1988 is coordinated by the Ministry of Foreign Affairs. Recently, the ministry developed guidelines for terrorists listing and de-listing procedures, which, however, were not yet in force at the time of the on-site visit. To date, no person or entity was proposed for designation by the Czech Republic to these UNSC Committees. In absence of any practical examples, the effectiveness of the mechanism in place could not be assessed.

289. UNSCR 1373 is implemented by the Czech Republic through the EU Regulation 2580/2001. At the time of the on-site visit the CzR did not have clear procedures or channels to make proposals to give effect to the actions initiated under the freezing mechanism or receive direct requests from foreign country pursuant UNSCR 1373. The assessment team was advised that in practice, the Act on Implementation of International Sanctions (IIS) would be used for these purposes and the FAU would be an institution through which such request could be made. Nevertheless, in absence of any practical example, the effectiveness of such mechanism could not be assessed.

290. Designations under the UN and EU are communicated to the REs and the public by posting the sanctions lists on the FAU's official website[38] (information on UN listings is archived after the new designations are taken over by the EU[39]). The timeframe for publishing new designations on the FAU's official website is, on average, 1-2 days. Whilst the information on new designations is published by the FAU regularly, the same approach is not applied to the information on amendments to the existing designations. The absence of information on amendments raises doubts on the overall accuracy of the information on UN designations published on the FAU website.

291.The FAU distributes information about the new UNSC designations to the financial institutions via MoneyWeb. Some DNFBPs, individuals and entities, receive this information via e-mail, upon subscription to the FAU website. Although the FAU is partially able to ascertain the coverage of entities receiving its newsletter through the e-mail addresses of the subscribers, it has not determined what percentage of the reporting entities has actually subscribed. Thus, the uneven approach towards the FIs and DNFBPs, on distribution of information, together with the uncertainty on the subscription coverage by the reporting entities, casts doubts on the effectiveness of the TFS communication mechanisms in place.

292. Banks, insurance companies, investment firms, and money or value transfer services met onsite rely on the internationally recognised commercial databases (most commonly - World Check) to screen their existing and potential customers against the sanctions lists. Moreover, some of them update their databases incorporating new information on designations received from the FAU. Clients are checked against the TFS lists at the stage of establishing the business relationship, and in every occasion when transactions are carried out. Regular checks of client database are automatically performed on a weekly basis, on average.

293. Overall, based on the interviews with the respective supervisory authorities and reporting entities, the assessment team concluded that banks and investment companies have better understanding of their responsibilities related to implementation of UN and EU TFS when compared to other financial institutions. Those interviewed on-site demonstrated substantial awareness on the matter – the scope of persons to be screened not limiting them only to the persons and entities

[38] http://www.financnianalytickyurad.cz/mezinarodni-sankce/aktualne-o-sankcich.html

[39] http://www.financnianalytickyurad.cz/mezinarodni-sankce/archiv-sankci.html

directly listed, but including the detection of assets owned or controlled directly and indirectly by the listed persons and entities. These institutions also demonstrated the abilities to analyse and independently decide in cases when they identify partial matches between their clients' details with the data reflected in the TFS lists. This practice was not confirmed by other FIs, since they exclusively rely on automated screening systems. In addition, they were not aware of other measures to be applied once funds or other assets jointly owned or controlled, directly or indirectly, by designated persons or entities or of persons acting on behalf of, or at the direction of designated persons or entities, are detected.

294. Different DNFBPs also demonstrated different levels of understanding of their responsibilities related to implementation of UN and EU TFS. Notaries, casinos, auditors, part of tax advisors and real estate agencies use built-in screening software which is directly connected to the websites of the EU and the FAU. These reporting entities advised that they check the clients against their database before establishing a business relationship. Moreover, notaries confirmed, that the same screening requirements are applied to their clients prior to conducting any transaction, while the tax advisors said that they conduct checks with those clients with whom they have an on-going business relationship on a yearly basis.

295. Lawyers, dealers in precious metals and stones (DPMS) and one of the tax advisors met on-site, stated that they check their clients against the EU sanctions list only. For this purpose they use the EU sanctions website. DPMS met onsite advised that they receive the FAU updates on the sanctions lists, which, however, are not accompanied by any instruction. Furthermore, the interviews held on-site confirmed that these reporting entities do not conduct checks of their clients with whom they have an on-going business relationship.

296. With regard to measures in place for identification of the BO aiming at identifying persons indirectly controlling or owning the assets involved in transactions, there are certain doubts whether some FIs (apart from the banks and investment companies) and DNFBPs are able to effectively establish the BO structure. In particular, and as described in IO 4, reporting entities, while performing a CDD process, over-rely on customer's "solemn declaration" and data kept with the Public Register. No further, independent, checks are carried out. At the same time, and as described in IO5, concerns are in place whether the accuracy of BO data maintained in the Public Register is reliable given the deficiencies of data gathering and their verification (see also IO4).

297. The FAU advised that they regularly meet the FIs and DNFBPs to discuss their TFS related obligation. The 'red flag' indicators were developed for the REs to detect FT suspicions. Nonetheless, this document was not yet been formally adopted and disseminated to the obliged entities by the time of the onsite visit.

298. In February 2018 the CNB developed the Supervisory Benchmark 2 on Requirements for Selected Procedures for Implementing the International Sanctions. This document provides an overview of legislation on international sanctions, requirements and expectations of CNB with regard to application for the international sanctions by the financial institutions. However, the financial institutions met on-site were not aware of this document. No guidance has been developed for the other types of reporting entities.

Targeted approach, outreach and oversight of at-risk non-profit organisations

299. Within the NRA framework, a special working group was established to review the NPO sector related FT risks, assess its potential vulnerabilities and develop mitigating measures. The working

group consisted of representatives of different ministries[40] and LEAs. A separate chapter of the NRA is dedicated to the analysis of NPOs sector vulnerabilities, and threats related to FT. Overall, the NRA assessed the risk of NPOs exposure to FT as serious[41]. The bases for the analysis were the legal framework and potential cases of NPOs' abuse for FT purposes. The NRA has identified all NPOs as falling under the definition provided by the FATF standards and has applied a generic approach towards the whole sector. The authorities explained that this conclusion was drawn based on the fact that, as per the Czech legislation, all NPOs are entitled to organise public fundraisings. However, the assessors deem that while assessing the risks covering vulnerabilities of the sector the CzR has not based the analysis on the characteristics and activities, neither on the subset of the NPOs actually organising fundraising. The NRA also assessed the vulnerabilities of the legislative framework specifically targeting transparency and record-keeping requirements, while also stating that sufficient mitigation measures were taken in the form of legislative amendments. At the same time, it does not assess NPOs sector vulnerabilities connected with the absence of risk-based supervision.

300. Since no case of NPO misuse for FT purposes has been identified in the Czech Republic, the NRA provides only hypothetical examples of FT abuse. These examples include FT abuse mainly through "*potential influence of foreign actors on radicalisation of individuals or respective groups, or transfers of foreign hazardous non-player characters' activities to the CzR*". On the other hand the NRA did not include any hypothesis of abuse resulting from the legislative and institutional gaps (e.g. abuse of unregistered churches) present in the Czech Republic.

301. There are currently 115.083 registered NPOs[42] in the Czech Republic, 91% of which are associations. Most of their funding comes from state subsidiaries, the EU and USAID grants or through the NPOs own fund raising activities. A small portion of NPOs operates abroad, including in the conflict zones, where they provide humanitarian aid. These are mainly branches of worldwide well known organisations (UNICEF, People in Need, etc.). Their activities include distributions of food kits and cash vouchers of about 200 euros. Controls are in place to ensure that the aid is used for the purpose it was provided via engagement of distribution and post distribution monitoring by the NPOs themselves and sometimes by the donors. For this purpose, the beneficiaries receiving (above 1000 euros) and the donors providing (above 200 euros) donations are checked against sanctions lists (mainly EU, US and UK) by teams which involve representatives of both the NPO and the country where the charities are directed to.

302. The Government Council for Non-Governmental Non-Profit Organizations (RVNNO) is a permanent consultative and coordination body of the Government for the NPOs related matters. Among other activities, the Council holds meetings with the relevant state authorities to discuss the matters of importance in this particular field, including policies of subvention from the state budget, the process for subsidy award and use, etc. Several meetings on FT related matters were also organised for the NPO sector by the RVNNO with the involvement of MFA, relevant supervisory authorities and the FAU. Apart from this, the FAU has held several seminars on threats of abuse of NPOs for FT purposes for reporting entities. In addition certain scenarios on potential NPOs abuse for FT purposes are elaborated provided on the FAU's official website.

[40] Ministry of Interior, Ministry of the Justice, Ministry of the Foreign Affairs, relevant departments of the Ministry of Finance and Ministry of Culture) and law enforcement authorities (Police) and FAU and Tax Administration and the Government Council on NPOs.

[41] The attributed risk levels in the Chapter 4.1 of the NRA range from *serious to moderate and to not significant.*

[42] Foundations, associations, religious legal persons, endowment, institutes, public benefit companies, professional association of legal persons, labor union, employers organizations, political parties and movements, churches, religious companies and hunting associations.

303. Notwithstanding the information made available on the FAUs website, together with a workshop on outcomes of the NRA organised for the representatives of the NPO sector, the interviews held on-site could not confirm that the overall level of their awareness of the CFT legislation and the NRA findings is satisfactory. In addition, their awareness on possibilities of them being misused for FT purposes was very limited. Most of the action to raise awareness in this field results from initiatives by the international NPOs headquarters, or by their donor organisations (EU, USAID, etc.).

304. Financial transparency and record-keeping requirements set for the NPO sector (as provided under R.8) are numerous. The NPOs are obliged to publish their annual reports and financial statements. The supervision on NPOs record-keeping is performed by the Registry Court under the auspices of the Ministry of Justice and Ministry of Culture. Although the registered legal persons are obliged to communicate to the Registry Court all necessary documents and information, the interview with the Ministry of Justice representative confirmed that most of information held by the Registry Court is not up to date. The Registry Court does not monitor the quality and accuracy of information submitted by the registered entities, and what the Court does check is only whether all required information is submitted. In such cases they contact the organisation and ask for the missing data. Fines can be applied against NPOs, when they fail to provide the required information, which can also result in their dissolution in case they repeatedly fail to provide such information. As stated by the authorities, it rarely happens in practice that the courts receive information on inaccurate information and then take further actions. No information/statistics on actual breaches identified and sanctions applied was provided by the Czech authorities, thus the effectiveness of this mechanism remains unclear.

305. Religious organisations and churches are supervised by the Ministry of Culture. All the registered religious organisations are, as per the requirements established by the law, also the accounting units and are obliged to keep their financial records. At the same time, churches have the right to decide whether they want to obtain legal personality through the registration or not. If the church is not registered, it cannot exercise certain rights i.e. it cannot apply for public grants or receive or distribute funds via bank transfers, etc. However, there is no legal limitation for the church to receive donations in cash. These donations could be transferred to its members via bank transfer, whilst the decision of their further use is afterward made by the relevant church's councils. Also, if the church decides not to be registered, there is no requirement for them to submit relevant information to the Ministry of Culture, and ultimately no supervisory action can be applied. Although the authorities advised that in practice no case of abuse of churches for FT or any other crime was noted so far, the situation as it stands at the moment, with no strict requirements for registration and consequently no supervision, raises concerns as to the probability of them being abused, inter alia, for FT purposes.

306. Financial statements published by the NPOs are checked by the Tax Administration, a supervisory authority for auditing accounting documents for tax purposes. Whenever state subsidies are provided to the NPOs, the Ministry of Finance supervises the consistency of their use with the declared purpose, and conducts ad hoc checks of donors and recipients of donations. The practice revealed that the main violations identified so far concerned improper record-keeping.

307. Notwithstanding the supervision carried out by the aforementioned authorities, none of the state institutions carries out checks which would target potential abuse of NPOs for FT purposes. While different authorities have access to information on NPOs' financial activities, it appears that there is no streamlined and targeted policy, neither coordinated interagency approach with regard to application of the risk-based supervision of the NPOs with respect to the FT matters.

Deprivation of TF assets and instrumentalities

308. As provided under the TC Annex, the Czech legislation does not set appropriate mechanisms for deprivation of the FT related designated person's assets (see also Recommendation 6).

309. A total number of 17 STRs (16 by banks and 1 by a bureau de change) were submitted to the FAU on FT suspicion, all of which were discussed with the LEAs. The discussions and subsequent analysis could not confirm any FT. Consequently, no investigation was initiated based on STRs. No positive matches were identified with persons designated under the relevant UNSCRs and no freezing of assets and instrumentalities of terrorists, terrorist organisations or terrorist financers were applied. In the event of locating funds or other assets, authorities were confident that funds would be automatically frozen as soon as a STR is filed with the FAU. While recognising the FAU's initiative to properly aware reporting entities on the importance of the matter, the opinion of the assessment team is that immediate freezing of funds or other assets is rather questionable given the deficiencies identified and elaborated in the text above.

310. At the same time, the assessment team is concerned that the deficiencies related to the STR filing process (in relation to the role of SRBs of some DNFBPs as provided under IO.6), together with other deficiencies identified in the TC Annex (notably the limited definition of the property that can be suspended under the national legislation vs. the EU legislation), may also hamper the effectiveness of the system in place. Furthermore, a contradiction between the approaches by the authorities and these of the reporting entities also supports such a conclusion - whereas the former said that the EU regulations would prevail when applying TFS (triggering application of freezing actions towards a broader definition of property), the latter advised the assessment team that they relied exclusively on national legislation.

Consistency of measures with overall TF risk profile

311. The assessment team identified that Czech authorities have made considerable efforts to analyse the FT risks. Due to the applied approach in assessing the risks the NRA does not provide an overall FT risk rating. It rather suggests that, on one hand, from the point of view of its seriousness, the FT poses a high threat, while, on the other, there is a low probability of its occurrence (for more detailed analysis please also see IOs 1 and 9). This notwithstanding, the authorities met on-site demonstrated good understanding of the FT threats, whilst certain measures to mitigate these threats were either implemented or their implementation was underway. In particular, the Czech Republic already took steps to improve its legal framework for implementation of TFS – a national mechanism for designation of persons and entities has been developed. However, this important legal instrument was not yet approved at the time of the on-site visit.

312. As concerns the consistency of measures with the FT risk in the NPO sector, as was indicated above, while the risk of NPOs exposure to FT is assessed as serious, there is a room for improvement in identifying country specific risks. The Czech Republic based the analysis of FT related risks on hypothetical cases of NPOs abuse, rather than analysing the exposure to threats by the specific types of NPOs e.g. those which actually organise and do raise funds through fundraising activities. Whilst the assessment team acknowledges the efforts by the authorities to perceive and subsequently raise awareness on potential cases when NPOs can be abused for FT, obliged entities met onsite lacked awareness on the level of NPOs exposure to FT risks. In particular, while the NRA identifies the level of NPO sector exposure to FT being high, no unified approach has been adopted by the obliged entities towards this sector. Furthermore, the measures proposed in the NRA are general – e.g. "*prohibit the establishment of entities aiming to violate the law and decide on their cancellation…"; "collect information and investigate suspicion*" which does not allow proper conclusion on their adequacy.

313. Overall, the evaluation team has concluded that the measures taken by the authorities with respect to prevention of terrorism related persons and entities from raising, moving and using funds and abusing the NPO sector, are consistent with the Czech Republic FT risk profile only to some extent.

Conclusions

314. The CzR has established a domestic mechanism to implement the UNSCRs, which, does not ensure the timeliness in implementing the related TFS. However, this mechanism may, to some extent, prevent terrorists from raising, moving and using funds. The Czech Republic has no domestic mechanisms apart from ones developed under the EU framework for implementation of the UNSCR 1373 to directly cooperate with foreign jurisdictions to give effect to action under the freezing mechanisms. Certain shortcomings are identified with respect to communicating the designations at a national level.

315. Larger FIs, such as banks and investment companies have better understanding of their TFS related obligations as compared to other financial institutions and DNFBPs.

316. Risk assessment of the NPO sector carried out as a part of the NRA, failed to identify a specific subset of NPOs being vulnerable to terrorist abuse, applying a generic approach to the whole sector of NPOs. Nevertheless, the country has made positive steps aimed at increasing the transparency of the NPO sector by amending the legal framework to prevent their abuse for FT. Currently, the supervision of the NPO sector is mainly tax-oriented, while there is no risk-based supervision on FT. The level of understanding by the NPO sector of their risk of FT exposure is not satisfactory.

317. Technical deficiencies noted under R.6, as well as the issues related to STR reporting have some negative impact on the effectiveness of CzR's sanctions regime. **Overall, the CzR has achieved a moderate level of effectiveness for Immediate Outcome 10.**

Immediate Outcome 11

318. The CzR is exposed to risks of proliferation financing since it has an advanced manufacturing economy, which includes a number of industries, including those which produce military and dual-use goods. In general, the authorities demonstrated a high level of awareness and understanding of proliferation risks. They have set up adequate co-operation between the customs and other export control authorities, which also entails co-operation with the security services.

319. The CzR has in place a robust system for licensing and export controls on proliferation-sensitive goods. The country is a member of the main international export control regimes in this area, including the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies. It is a signatory to a large number of international instruments, among which is the Treaty on the Non-Proliferation of Nuclear Weapons. The authorities duly submit their country reports to the UNCSR 1540 Committee, the last one being handed over in 2016.

320. The assessment team was informed that, as far as Iran is concerned the Czech Republic has a dual-used goods trade licensing experience (e.g. 13 licenses for export of dual-use goods to Iran were issued in 2016). With the Democratic People's Republic of Korea (DPRK) the Czech Republic has no formal trade agreements.

321. As a reflection of the CzR's role in the Neutral Nations Supervisory Commission (established under the 1953 Korean Armistice agreement), the country hosts the DPRK Embassy. The embassy was permitted to open a bank account to ensure the funding of the premises and mission in line with

the UNSCR 2321 (2016) implemented through (ES) 329/2007. Yet the CzR authorities advised that the account had not been opened at the time of the on-site visit.

Implementation of targeted financial sanctions related to proliferation financing without delay

322. As a member of the EU, the CzR applies the EU framework for implementing designations under respective UN Security Council Resolution on the PF TFS, which consequently affects the Czech Republic's ability to effectively implement relevant UNSCRs without delay.

323. The EU mechanisms do not suffer from technical problems in relation to the time of their transposition when it concerns Iran. Individuals and entities had already been listed by the EU when their designation by the UN was made. Moreover, the EU applies sanctions to a significant number of entities that are not designated by the UN. There are additional mitigating measures applied by the EU requiring a prior authorisation of transactions with Iranian entities. This allows the authorities to determine if the transfer of funds for which the authorisation is requested is in breach of any of the prohibitions or obligations stipulated by the EU Regulations.

324. As for the TFS against DPRK, in the past, some designations by the UN were shortly transposed into the EU framework. Nevertheless incorporation into the EU legal framework[43] of the most recent additions made to the UN list of designated persons and entities (of 02 June 2017, 05 August 2017, 11 September 2017 and 22 December 2017) took 8 days, 6 days, 5 days, 4 days and 17 days respectively. Hence, despite recent improvements, delays in implementation of the UNSCRs of DPRK still occur.

325. At the national level the Czech Republic has developed Methodological Instruction 5 aimed at ensuring a proper implementation of UNSCRs prior to transposition of new UN designations into EU framework. As explained under IO 10, this mechanism does not set an obligation to freeze assets on the basis and for the duration of the validity of the UNSCR decision. Nevertheless, the authorities indicated that the funds would be further suspended by virtue of application of the AML/CTF Act (Article 20), i.e. the obliged entities would not proceed with the transaction within 24 hours after submission of the STR, waiting for the FAU decision of suspension of transaction or seizure of assets, thus preventing terrorists from raising, moving and using the funds.

326. When it concerns the communication of designations to the reporting entities, it shall be noted that the latest designations under UNSCR 2270 were published by the FAU on its website and also communicated via MoneyWeb five days after the designation by the UN. This cannot be considered as an immediate communication of TFS related to PF.

327. Considering that the Methodological Instruction 5 is equally applied for both, proliferation financing and FT, and taking into account that the same way of communicating new designations is executed by the FAU for both PF and FT, the analysis on these matters provided under IO 10 also applies to IO 11.

328. As for national level coordination in countering PF, limited information was provided by the authorities. They have indicated that there is a non-formal inter-institutional working group[44], which

[43] The EU sanctions database includes UN designations which are not yet implemented via EU regulation (with a specific indication of them being pending).

[44] The Working group is attended by the FAU, Ministry of Foreign Affairs, Ministry of Interior, General Customs Directorate, Ministry of Industry and Trade, State Office for Nuclear Safety, Ministry of Transport and Ministry of Education, Youth and Sport.

gathers relevant policy makers and operational authorities in this matter. The group meets quarterly or on ad hoc basis to discuss issues related to this area (see also IO 1).

Identification of assets and funds held by designated persons/entities

329. In the Czech Republic the private sector has yet not identified assets and funds held by individuals or entities designated pursuant to the PF TFS. On the other hand and as a result of effective co-operation and co-ordination among the General Customs Directorate, the FAU, Bailiff's office and the Ministry of Foreign Affairs, assets were identified and frozen pursuant to the UNSCR 1718. This case demonstrates that authorities have capacities to properly implement TFS where an asset related to a PF designation is identified. Details of the case are presented below.

Case on freezing of assets related to DPRK

In 2012 the FAU received a request from the General Customs Directorate regarding goods stopped on the borders of the Czech Republic coming from the Democratic People's Republic of Korea. This delivery contained several computer numerical control machines and was accompanied with documentation from the Korean company. Based on this information the FAU asked the Czech company which was the recipient of these goods to provide additional information about the trade and also asked the Ministry of Foreign Affairs about the status of the Korean company (its name figured on the invoice and the shipping documents). The FAU also inquired about Korean company's potential linkage with the DPRK company which name figured on the labels of the goods. Whilst the company which was the direct exporter was not in the sanctions list, the company which name figured on the label of the goods was designated by the UN.

Consequently, the FAU issued a decision on freezing of funds of a total amount of USD 105.600 of the Czech company to prevent the payment of goods to DPRK.

Even though the decision on freezing of funds was acknowledged by the Czech company, it failed to deliver the funds to a special bank account on time. The FAU contacted the Czech company but the communication did not lead to any agreement to proceed as the FAU had previously decided. The bailiff's office froze all moveable and immovable property of the Czech company and initiated a dialogue on further process with its representative. Funds generated by the property of this entity were deposited on the account. The FAU then forwarded the case to the court bailiff who executed the decision. The FAU also imposed a fine in line with the IIS Act for breaching the obligation to deliver funds for which the freezing order was made.

330. Based on the case described above, the Czech Republic initiated further steps and proposed designation of the above-referred DPRK's company (the one which was a direct exporter) before the UNSC Committee established pursuant to Resolution 1718. This proposal was approved by the UNSC Committee and resulted in designation of the entity. Some details concerning the designation provided by the authorities are summarised in the box below.

Case on designation of an entity pursuant to UNSCR 1718

The FAU, in cooperation with MoFA, prepared a proposal for designation to the UN Security Council Committee. Prior to rendering the proposal, assets of the Czech company of a total amount of USD 105.600 were frozen by the FAU. The proposal was based on paragraph 8 letter d) of the UNSCR 1718 (2006) and was presented by the Permanent Mission of the Czech Republic to the UN. The proposal included the relevant details about the company proposed for designation, evidence of possible linkage that the company had with the designated entity and the description of the particular situation. In January 2013, the proposed entity was listed pursuant to the respective UNSC Resolution. The designation of the same entity was also made under the EU framework.

331. So far, no STR has been submitted related to PF by reporting entities[45] to the FAU directly or via the respective SRBs' chambers. Similarly, except for the case described above, no freezing of assets and instrumentalities of proliferation of weapons of mass destruction has been applied. Hence, there was no practice of application of measures with respect to unfreezing of funds or granting exemptions. At the same time, the assessment team, as also elaborated under IO10, is concerned whether the reporting entities' obligation which regards the deprivation of PF assets from their clients (or potential clients), is applicable in practice.

332. In addition, the issues raised under IO10 in relation to shortcomings identified in the mechanism for STR reporting, the role of SRBs in this process and the limited definition of property subject to freezing under national legislation similarly affect the effectiveness with regard to IO11.

FIs and DNFPBs' understanding of and compliance with obligations

333. There is an uneven level of understanding of PF-related TFS obligations among the reporting entities. Banks and larger FIs demonstrated a good level of understanding of their freezing obligations. These institutions use commercial databases to screen their clients. However, in case of non–bank FIs, screening of their clients is usually done on a weekly or monthly basis. Other reporting entities have almost no awareness of UN sanctions regime related to the PF.

334. DNFBPs lack understanding on PF and their obligations towards implementation of the TFS. Most of them do not screen their clients against the sanctions lists. In addition, these DNFBPs which perform screening and thus potentially detect a sanctioned entity or person, in case there is a match, would still carry out the transaction[46]. Only few reporting entities met on-site mentioned that they would consult the FAU or the respective SRBs chamber before proceeding with the transaction. The potential for sanctions evasion, including through the use of persons or entities owned or controlled by those designated, is not widely understood, and the awareness of the dual-use goods regime is limited.

335. The reporting entities rely on national legislation only (not on the EU legal framework) in the course of their operations. Whenever there is a property to be frozen, the definition provided under the national legislation will be applied, which is narrower compared to the EU framework.

Competent Authorities Ensuring and Monitoring Compliance

336. The FAU, together with the respective supervisory authorities is conducting monitoring and ensuring compliance by FIs and DNFBPs with their obligations regarding proliferation related TFS. As stated by the supervisory authorities, implementation of TFS by the reporting entities, including presence of screening mechanisms, is a regular part of the onsite and offsite controls performed by the supervisors. Whilst the staff of the supervisory authorities receive regular trainings in TFS matters, the lack of human resources (highlighted under IO3), may have an impact on the effectiveness of monitoring the PF-related obligations.

[45] At a later stage of the evaluation process, after the on-site visit and the face to face meeting the authorities have informed the evaluation team that there was 1 STR submitted by bank in July 2017 with a suspicion that a client is involved in transactions breaching the TFS on Iran, which however was not further confirmed by the FAU, and 1 STR was submitted by bank in August 2017 with respect to Foreign Trade Bank of the DPRK, and as a result, the accounts were frozen. This information however is not reflected in the analysis due to the late submission, which made impossible to confirm the details with the private sector and all the relevant authorities.

[46] Namely, real estate agents, lawyers, notaries.

337. Authorities stated that several workshops and seminars for both reporting entities and exporters on proliferation financing were organised by different authorities. Nevertheless, most of the reporting entities lack clear understanding and guidance on their obligations. Not all the reporting entities could recall the discussions and issues elaborated during the awareness-raising seminars provided for them. As stated in IO10, in February 2018 the CNB developed the Supervisory Benchmark 2 on Requirements for Selected Procedures for Implementing the International Sanctions. However, the financial institutions met on-site were not aware of this document. No guidance has been developed for and provided to the other types of reporting entities.

338. Based on the interviews with the private sector and the supervisory authorities, it was evident that the lack of awareness among reporting entities had resulted in breaches of EU and UN TFS obligations. An example of such practice is provided below.

Case on breach of obligations by a bank

In 2017 the CNB conducted an on-site inspection of a bank. In line with the internal procedures a bank, clients who signed a long term deposit contract (for 2 and more years) were screened against the international sanctions lists at the stage of establishing a business relationship, and further, once a month. Meantime, clients using other types of services provided by the same bank were screened on a daily basis.

The CNB has analysed all the clients and transactions conducted in relation to these long term deposit contracts. The CNB detected that none of these clients appeared to be included in the lists of designated persons, and no deposit was withdrawn over the period when this service was provided.

The CNB discussed with a bank the appropriateness of the applied measures and subsequently requested application of corrective measure. A bank revised its internal procedures accordingly.

339. The CNB pays appropriate attention to the implementation of the TFS by the financial institutions, and applies appropriate technics to identify any funds made available to the designated persons. However, and as reflected under IO 3, the sanctions applied by the CNB do not appear to be proportionate to the identified breaches.

340. In a number of occasions (33-in 2012, 23-in 2013, 4-in 2014 and 5-in 2015) breaches identified concerned the lack of prior authorisation of transfers, as required by the EU Regulation 267/2012 on the Islamic Republic of Iran. These breaches triggered administrative proceedings with application of fines (24-in 2012, 22-in 2013, 2-in 2014, and 5 in 2015) based on the provisions of the IIS Act. The average size of the fine applied was approximately 20.000 CzK (800 EUR) The fine was calculated based on the amount of assets under consideration. The sanctions applied appear to be proportionate and dissuasive.

Conclusions

341. The CzR has established a domestic mechanism to implement the UNSCRs, which, however, does not ensure the timely transposition of the PF related TFS and their implementation without delay. However, this mechanism may, to some extent, prevent terrorists from raising, moving and using funds. Certain shortcomings are identified with respect to communicating the designations at a national level. The unclear procedures and lack of proper understanding of freezing obligations with regard to PF; shortcomings related to procedures for submitting the STRs; lack of guidance and dialogue between the authorities and the reporting entities on PF related matters resulted in number of breaches of obligations by the private sector.

342. It shall also be acknowledged that state authorities demonstrated their capacity to implement the UNSCRs, which resulted in identification and deprivation of assets from a company linked with

the designated entity. In addition, the country has also proposed an entity to be designated by the UN and this proposal was approved. The state authorities demonstrated the capacity to properly supervise the implementation of the UNSCRs, although concerns remain on the proportionality of the sanctions applied by the CNB. **Overall, the Czech Republic has achieved a moderate level of effectiveness for Immediate Outcome 11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

- Significant efforts have been devoted by the FAU to raise awareness on the findings of the NRA, to which the private sector contributed to a certain extent. As a result, most FIs in the Czech Republic broadly understand the main ML threats as derived from the NRA document.

- The banks have an appropriate understanding of the ML/FT risks and obligations, but awareness is lower with the other FIs. The DNFBPs awareness of AML/CFT risks varies - whilst certain professions demonstrate sufficient knowledge (auditors, notaries), some other (e.g. real estate agents) need improvements. The real estate sector in the Czech Republic has two particularities which render it vulnerable (the possibility to use crypto currencies at acquisition and the absence of an obligation to notarise the real-estates deeds), and the assessment team is not confident the associated risk is well understood and properly mitigated.

- The perception of the FT risks is based on the NRA, experience/group guidance, and guidance from the supervisors. The way the private sector can be abused for FT purposes is not adequately acknowledged by some DNBFPs.

- FIs and DNFBPs generally demonstrated a good knowledge of the AML/CFT requirements, but the risk-based approach is applied almost exclusively by banks, securities intermediaries and insurance industry. The mitigating measures are generally taken according to the perception and understanding of risks across the sectors, which is not always consistent with the materiality and the context on the ground.

- The CDD regime is generally in place, the FIs/DNFBPs may decide not to establish business relationship in certain cases, and do not enter in a business relationship in case the client refuses identification. The reporting entities do identify the persons acting on behalf of their customers. Nevertheless, the verification of the BO is often overly reliant on client's "solemn declaration" and/or data obtained from the Commercial Register. Similar principles are applied when understanding and verifying the source of funds.

- Banks and insurers routinely check their prospective and existing clients against various databases to identify or verify potential PEPs. The rest of the financial sector and most of the DNFBPs have insufficient understanding of the significance of PEPs and the associated risks. There is a general agreement that corruption remains an issue in the country, but its connection with the AML/CFT regulations related to PEPs is not always understood.

- According to the FAU the quality of STRs increased significantly in the last couple of years. The Czech banks are the main contributors in terms of STR submission, while the volume of STRs submitted by the DNFBPs is commensurate with their limited awareness in the ML/FT area.

- While banks and large financial institutions have adequate level of internal control procedures, DNFBPs and small financial institutions fall well short of the desirable standards in this regard.

Recommended Actions

The Czech authorities should:

- Amend legislation to address the technical deficiencies described in the Technical Compliance Annex. In particular, they should amend the AML/CFT Law to include an explicit requirement to perform ECDD in high-risk scenarios (including for PEPs);
- Clarify the discrepancies between the AML/CFT Law and the FAU Instruction nº 7 on the issue of foreign and domestic PEPs[47];
- Intensify and enrich the trainings provided to non-banking financial institutions (especially payment service providers and currency exchangers) and DNFBPs on ML/FT risks and respective mitigating measures to further clarify that the DNFBPs should assess their entity wide risks, risks arising from their products and customers. When assessing the risk the NRA, relevant guidance, typologies and feedback from the FAU should be taken into account.
- Enhance awareness of currency exchangers, securities sector and DNFBPs (especially gaming industry) with regard to PEPs and the correlation with the corruption risks;
- Take measures to mitigate the particular ML related vulnerabilities which concern the real estate sector;
- Provide specific CTF trainings to all reporting entities;
- Take measures (such as awareness raising) to improve business practices (such as accessing more publicly available sources) of reporting entities (especially DNFBPs)so that they are not overly reliant on the customer's solemn declaration on beneficial ownership, PEPs and origin of funds;
- Take measures (by e.g. providing targeted trainings and guidelines) to improve quality and volume of STR reported by DNFBPs (especially currency exchangers and real estate dealers).
- The authorities should consider granting private sector entities access to a selected number of data bases managed by public bodies. The access should be given based on risk and on the need-to know principle.

Immediate Outcome 4 (Preventive Measures)

343. Since the adoption of the 4th round MER, the Czech Republic has made important legislative and institutional reforms to strengthen its AML/CFT system. Some of these reforms (most notably the adoption of legislation on the Registry of Beneficial Owners) will yield benefits in the future.

Financial Institutions

344. The banking sector is by far the largest financial service provider in the Czech Republic. The rate of Financial Inclusion is quite high – 82%[48]. There are 58 banks in the Czech Republic, which have the following ownership structure:

Ownership structure of banks in June 30, 2017		
	Number	**Value of assets (EURO[49])**
Foreign ownership more than 50%	18	EUR 225,2 bn

[47] The authorities advised that in April 2018 the FAU issued an up-date of Methodological Instruction 7 to render it more in line with the requirements of the AML/CFT Act.
[48] http://datatopics.worldbank.org/financialinclusion/country/czech-republic
[49] Exchange rate as of June 30, 2017

Foreign ownership less than 50%	0	
Resident Shareholders 100%	15	EUR17,1 bn
Foreign Branches	25	EUR 23,3 bn
Total number of banks	58	EUR 265,6 bn

345. The prevailing majority of the bank assets are held by non-residents. The largest foreign-owned banks have parents in the western European countries[50]. Natural persons account for 94% of the bank customers while legal persons are at 6%. Non-resident customers hold 10.2% (non-Czechs EU citizens and non-EU citizens) of total customer assets in the banks. The EU customers constitute 97% of total customers in banks, while 3% of customers are from non-EU jurisdictions.

Understanding of ML/TF risks and AML/CTF obligations

346. The representatives of banks met on-site demonstrated a proactive approach to risks and good understanding of their AML/CFT obligations. Banks do not use the Czech NRA as the unique source for their risk analysis, but also consider the EU Supra-National Risk Assessment, public sources, their own experience, and group-wide assessments. They identify: (i) product-related risk (e.g. mortgage, credit loans, letter of credits), (ii) customer-related risks (e.g. non-resident customers, PEPs) and (iii) transaction-related risks based on potential predicates typologies (i.e. tax evasion, frauds, phishing schemes). Risks are classified into "low", "moderate" and "high" categories, and specific mitigation measures are taken accordingly. The risk assessments are updated periodically (yearly), and when significant changes occur in the course of business (i.e. new products are launched on the market).

347. Most of the banks met on site employ sophisticated software tools to analyse risks and detect ML/FT indicators, incorporating numerous scenarios. The software allows for online checks against various open sources and databases and feed the findings into the risk management system (i.e. identification of PEPs, sanctions list etc.). Securities intermediaries rely mostly on the findings of the NRA.

348. The life insurance industry recognises the AML/CFT risk when related to geographical location of the customer, corruption and PEPs. The insurers developed a system of indicators based on behavioural patterns of their customers which would indicate a higher risk and trigger the submission of STRs.

349. Payment service providers document their ML/FT risk assessments based on categories of risks prescribed in the law or from the guidance given by the FAU. They were able to demonstrate a sound understanding of their legal obligations and explained what type of customers pose a higher ML/FT risk. However, when questioned, they were not able to articulate why such persons presented a higher risk.

350. The currency exchange providers are sufficiently aware about the ML threats in their business and were able to detect some sector-specific vulnerabilities such as smurfing or customers exchanging EUR 500 banknotes. On a less positive note, significant difficulties were detected in relation to the understanding of risks and obligations related to PEPs.

[50] http://banksdaily.com/topbanks/CzechRepublic/total-assets-2015.html

351. The real estate sector in the Czech Republic has two particularities which render it vulnerable to ML/FT risk: (i) property can be and is sold for crypto currencies and (ii) the real estate deeds do not need to be notarised to be valid. Formalistically, the industry recognises corruption, tax crime and clients coming from certain countries as bearing ML risk and mentions cash transactions or inadequate market price as ML indicators. However, the assessment team is not confident that the associated risk is well understood and/or appropriate measures are applied (see also IO.1).

352. There are almost 300 land based and one online casinos in the Czech Republic. Casinos perceive AML/CFT risks as being related to cash operations, corruption and tax crimes, but in practice limited mitigation measures are taken. The AML/CFT obligations are often mixed with the anti-fraud policy of the establishments.

353. The understanding of AML/CFT risks, as well as the acceptance of the NRA findings amongst the other DNFBPs varies, but they rarely apply a risk based approach to their AML/CFT measures, and the majority does not monitor their customers on an on-going basis.

Application of mitigating measures commensurate with the risk

354. Czech financial institutions broadly understand their AML/CFT risk-based obligations and apply mitigation factors accordingly. The private sector is aware that enhanced measures must be taken in the areas of increased risks including: obtaining and analysing supplementary documents on the nature of the business, source of funds invested and origin of the wealth, more frequent scrutinising of transactions, etc.

355. The on-going monitoring regime is employed based on the customer's risk profile. In most of the cases, the banks perform automatic screening of their existing customers (on daily basis) to adjust their categorisation and identify potential clients who have been listed (on the UN sanctions lists for instance), or who became a PEP after the inception of the business relationship with the bank.

356. Risk-based decisions are taken by a number of financial intermediaries to restrict or exclude some business lines according to the risk appetite set in the AML/CFT internal rules. For example, there are some banks which do not provide products or services to crypto-currency operators (e.g. Bitcoin) or online gambling operators. Simplified measures are applied when the risk is less important.

357. At the inception of a business relationship, the securities intermediaries assign the clients in a certain category of risk according to a set of indicators (usually two categories are used: high-risk and low-risk). Subsequently, automated on-going monitoring based on algorithms is performed. In case of higher risk clients, the company provides investment counselling and usually this implies going into details in establishing the source of funds. Less attention appears to be paid to identification of potential PEPs clients.

358. The casinos fully identify their clients at entering in the premises. Following the identification, the customers are attributed with "player's accounts", which do not function as bank accounts, and incoming transfers cannot be made. However, at client's request, casinos can transfer the winnings into client's bank account. The customers are not categorised according to the risk, and PEPs are identified only if they declare themselves as such in the entry questionnaire. No subsequent verifications are performed. The only risk-based measure identified by the evaluation team was that crypto currencies are not accepted as a payment method.

359. Notaries have a sufficient level of awareness on ML/FT risks and understand their basic obligations. An example of a risk-based measure is the application of an enhanced monitoring over

escrow accounts through verification of the source of money, and additional information required from the clients.

360. The lawyers indicated that their ethical standards (rather than AML/CFT obligations) would require them to decline certain transactions and they seem to always perform KYC and basic AML measures. The risk related to the incorporation and management of corporate vehicles is recognised, but little risk-based measures are taken in this respect. The auditors are the most knowledgeable DNFBP in the AML/CFT area, while some of them also provide AML/CFT consultancy.

361. Enhanced measures are taken in relation to the NPOs which, based on international guidance, are generally recognised as posing a higher FT risk[51]. Otherwise, the FT risk is considered to be low and the DNFBPs take minimal measures for its mitigation.

Application of CDD and record keeping requirements

Financial Institutions

362. Financial institutions are generally familiar with their CDD and record keeping responsibilities. In the majority of cases, when opening accounts, clients must be physically present at the bank, present their IDs, fill in the questionnaires describing the nature of their business, source of funds and wealth, and provide relevant documents and contracts. This information is used to establish a profile of the customers against which their on-going activities will be monitored. If the provided data is incomplete, the bank refuses to cooperate with the client. In most of the banks, non-face-to-face identification (i.e. at check points) is accepted for approximately 1% of customers, who are considered low-risk.

363. In the verification process, the banks have access to several public and restricted databases (such as the criminal records, paid international databases). However, not all the databases held by the Czech authorities are fully used, one example being the database of stolen ID, which would be very relevant for e-banking oriented FIs.

364. E-banking operations, which involve remote opening of accounts, are understood as particularly risky. In these cases, as a prerequisite, the copies of ID documents must be sent via post and e-mail, and the client must take a photo of himself at registration. In all such cases, the first payment must be made via another bank account which must be provided to the e-banking operator. Additional verification measures are taken, such as sending a letter to the customer's registered address, to ensure that the addressee is aware that a bank account is being opened on his/her behalf.

365. The issue of verification of beneficial owners remains a preoccupation throughout the financial sector. FIs are trying to find the most effective ways to proceed with the verification of the BOs. When ascertaining beneficial owner and source of funds, some banks do not go beyond customer's declaration or data from the Commercial Register.

366. Along with the face-to-face identification, one of the payment service providers uses the services of their contractual partner – the Czech Post, which is obliged entity according to AML/CFT Law. The Czech Post provides money transfer services as per contracts signed with the MVT partner. No particular areas of concern have been identified in relation to these operations.

367. The record keeping procedures appear to be adequate and the required documents are often maintained for periods longer than prescribed by the AML/CFT Law and the CNB regulations.

[51] A similar approach is present in the Czech NRA Chapter 3.3.2

DNFBPs

368. Casinos perform CDD on their clients at the entry in the premises and the identification procedure includes taking a photo of the customer, verification of validity of the documents, sometimes even fingerprinting. If a customer refuses to be identified, he/she is denied access to the premises.

369. Lawyers, notaries, auditors and tax advisors generally observe the CDD requirements, mostly due to their professional profile and type of services provided, rather than for AML/CFT purposes. When involved in sale/purchase of companies or companies' shares, lawyers will ask the customers to fill in a standardised form, and both parties of the deal are verified using the Czech registries (i.e. Commercial Registry), foreign registries or open sources. If the law firm is a member of an international group, they will coordinate with the EU partners or with the parent company for purposes of BO identification.

370. NRA recognises that the real estate sector is highly exposed and vulnerable to ML risks, and there are numerous independent reports confirming the trend[52]. During the on-site interviews, the sector demonstrated some understanding of basic CDD and record keeping obligations, but is overly reliant on customer's declaration in terms of beneficial owners and origin of funds.

371. Dealers in precious metals and stones (or other high value merchandise) are "de facto" excluded from the CDD obligations as they are forbidden to perform transactions in cash above 270,000 CZK (approximately EUR 10,300).

372. Overall, the DNFBPs validate beneficial ownership information almost exclusively based on customer's declaration or data from the Commercial Register, without a proactive verification.

Application of EDD measures

a) PEPs

373. According to the NRA, corruption is considered to be a high risk factor for the Czech Republic and therefore, the FAU issued the Methodical Instruction no 7 "On Politically Exposed Persons" which is applicable for all reporting entities. Whilst the AML/CFT Law does not distinguish between domestic and foreign PEPs, Instruction no 7 requires enhanced measures to be applied only to foreign PEPs (customers or BOs). In relation to domestic PEPs (in the understanding of the draft EU AML/CFT Directive which to date define EU nationals as "domestic" PEPs), and persons who have been entrusted with an important function in an international organization, Instruction no 7 requires the reporting entities to apply specific measures only where a risky business relationship is established. The assessment team is of the opinion that the provisions of Instruction no 7 are contradictory, diverge from the AML/CFT Law, and may create confusion amongst reporting entities regarding which measures must be taken[53].

374. The banking sector and the big non-banking financial institutions, are aware of the corruption risks, and do use advanced software linked to international databases (in one case a Czech database) to identify PEPs. Smaller non-banking financial institutions are less aware of the correlation between corruption as a social phenomenon and the concept of PEPs. They do not apply effective measures to identify PEPs, be it domestic or foreign.

[52] https://www.occrp.org/en/investigations/1666-azerbaijans-czech-enclave

[53] The authorities advised that in April 2018 (after the on-site visit) the FAU issued an up-date of Methodological Instruction 7 to render it more in line with the requirements of the AML/CFT Act.

375. The DNFBPs (especially the designated professions) would pay special attention to domestic PEPs when identified in the course of the business relation, but no mechanisms or risk mitigation measures are in place to routinely identify them and apply ECDD procedures.

b) Corresponding Banking

376. Whilst the AML/CFT Act does not specifically require that the obliged entities understand fully the nature of the respondent institution's business, the interviewed Czech banks providing correspondent services to other institutions, confirmed that the relevant measures were in place. The banks do request foreign respondent institutions to fill-out comprehensive forms, which include questions regarding respondent banks compliance policy. Verifications are done through special intelligence units and in some cases conference calls are organised with the responding banks. The Czech banks would not cooperate with shell banks and would not establish relations with a respondent bank which has insufficient AML/CFT legislation. The behaviour and profile of the customers of the respondent banks are monitored on a regular basis and they would directly influence the risk level of the banking relationship.

c) New Technologies

377. FAU issued Methodological Instruction 2 "On Digital Currencies" by which the obliged entities are required to consider any such payment exceeding EUR 1,000 as high-risk, and report transactions exceeding EUR 15,000 as suspicious. The FIU informs that some STRs reporting exceeding the stipulated amount have been submitted and led to further analyses.

378. New technologies (online banking, new payment products, digital and crypto currencies) are considered as high risk throughout the financial system, and generally adequate enhanced AML/CFT measures are taken. Some of the entities would not accept transactions with virtual currencies.

379. As a particularity, real estate can be purchased in the Czech Republic using crypto currencies[54]. As a mitigating measure the FAU issued Methodological Instruction 2 "On Digital Currencies" which advises the reporting entities to scrutinise any such transaction exceeding 1.000 euros and report as suspicious any such transaction exceeding EUR 15.000. The Czech authorities informed the evaluators that crypto-currencies related STRs have been received in practice: 46 in 2016 and 133 in 2017. Crypto-currencies related STRs have been received. The authorities advised that the phenomenon is still not developed and no actual ML case has been detected in relation to virtual currencies. However, further guidance, monitoring and awareness raising actions are needed to fully address the particular risk related to crypto-currencies and the real estate sector.

d) Wire Transfers

380. The EU Regulation 2015/847, came into force on 26 June 2017 and is directly applicable in the Czech Republic. It requires that data on the beneficiary is attached when wire transfer is performed. The banks, which evaluation team met on-site, demonstrated relatively good understanding of risks associated with wire transfers and assured that they do enquire about the purpose of the transfer and the source of funds. The institutions met during on-site visit stated that the customers were screened against the UNSCR lists. The Czech institutions mostly rely on their foreign counterparts with regards to checks of their customers against the UNSCR lists.

e) Targeted Financial Sanctions Related to TF

381. As an EU member state, the Czech Republic is directly implementing the relevant EU TFS, regime which does not fully comply with the FATF requirements. In order to overcome the time gap

[54] http://www.homehunters.cz/en/bitcoin/

between the publication of new designations by the UN and their transposition into the EU framework, the FAU introduced Methodological Instruction5. The Instruction, however, does not ensure freezing of assets of designated persons and entities for duration of the validity of an action initiated by the UNSCRs. Banks and investment companies have better understanding of their responsibilities related to implementation of UN and EU TFS when compared to other financial institutions. Banks use advanced software which enables online screening and updating of both EU and UN lists. Different DNFBPs also demonstrated different levels of understanding of their responsibilities related to implementation of UN and EU TFS. Real estate agents, lawyers, notaries informed that in case they detect a match with the list of designated persons and entities, would still carry out the transaction. Only few DNFBPs met on-site mentioned that they would consult the FAU or the respective SRBs chamber before proceeding with the transaction. No freezing following the application of TFS have been reported during the on-site interviews (Please further details under IO 10 and IO 11).

f) Higher-Risk Countries Identified by the FATF

382. Financial institutions are to a large extent familiar with the risks posed by the customers from and transactions from/to high risk counties. The conclusions of the institutions are based on supervisory guidelines and internal/group level inputs. The countries are classified into several risk categories and measures applied commensurate to the level of risks.

383. Some of the DNFBPs met on site are unaware of the FATF designated high risk countries, while the others have an approach often based on personal perception of "risky countries", which is not always consistent with the FATF lists. As a result, many DNFBPs do not know how to treat transactions made by customers from higher-risk countries identified by the FATF.

Reporting obligations and tipping off

384. The FAU is confident that the quality of Suspicious Transaction Reports has improved over years, and the evaluation team can confirm that the principles of reporting of suspicious activity seem to be broadly known by the entities represented at the on-site interviews.

385. On a less positive note, some of the reporting entities use a limited number of indicators as a basis for filing STRs and several DNFBPs stated that they prefer to coordinate with FAU before submitting a STR. The overall number of STRs increased since the last evaluation, as it can be revealed from the following chart:

Table 13: Number of STRs received by FAU from categories or reporting entities

Sector	2016 STRs		2017 STRs	
	ML	FT	ML	FT
Banks	2146	11	1195	5
Cooperative savings	15		17	
Insurance sector	28		22	
Post licences holders	19			
Securities sector	22		22	
Electronic money	1			
Payment services providers	89		33	
Investment firms	4		1	
Loans providers	10		7	

Currency exchange	10	1	6	
CNB	5		1	
Casinos	1		6	
Real estate agents	2		1	
Dealers in precious metals/stones, Notaries, Accountants, Trust and company service providers				
Lawyers			3	
Auditors/Tax Advisors	1			
Companies providing registered offices	1			
Emission allowances traders	2			
Virtual currencies	6		2	
Reports on misuse of the tax administration system	371		229	
FIU	59		39	
Others	122	22	60	16
Other criminal offences and Attempted transactions for FIs and DNFBPs				
TOTAL :	**2948**		**1665**	

386. The banks are the main contributors in terms of STR submission (more than 70%) whereas the number of STRs submitted by non-bank financial institutions and especially DNFBPs remains low. While the evaluators admit that contextually the highest volume of financial assets and financial transactions are held/performed by the banks, there are sectors where the ML/FT risks remain present, without this being reflected in the reporting behaviour. For example, the NRA states that lawyers, public notaries, auditors, accountants, tax advisors and real estate dealers remain vulnerable to ML/FT risks but very few STRs have been sent to the FAU by these DNFBPs. The evaluation team is of the opinion that this constitutes a significant vulnerability, especially in relation to the real estate agents, bearing in mind the particularities of the Czech market.

387. Few FT STRs have been filed by Czech banks, and only one by a bureau de change. The low level of reporting may be justified by the limited risk identified in the country but it appears that there is also an insufficient awareness of the non-bank reporting entities on FT indicators. As described under IO6, the obliged entities often consult the FAU prior to submitting a STR and in this context continuous education of the RE and prompt feedback is ensured. Feedback is also provided in the context of AML/CFT trainings and other meetings held with the REs, and through the FAU website. The feedback is considered as effectively provided and positively appreciated by the REs, and significantly contributes to the quality of STRs.

388. Banks seem to be familiar with the tipping-off prohibition principles. The FIs internal rules routinely contain provisions regarding the ban to disclose the fact that an STR or related information is being filed to the FAU. To prevent tipping-off in practice, some FIs implemented a system of limited communication between the front offices (who could tip-off the client) and the Compliance (in charge of the STR filing). Others underlined that from the inception of the relationship, the client is clearly informed that the bank can at any time, for any reason require additional information as a regular procedure, hence, the client will not be alerted in case additional information is needed, even

in the event of an STR. The CNB can impose up to EUR 10,000 on natural persons for tipping-off, but no such sanctions have been imposed so far.

Internal controls and legal/regulatory requirements impending implementation

389. Large financial institutions have an adequate level of internal control procedures, which is performed by the internal audit. According to AML/CFT Law, specific training must be provided to employees of reporting entities at least once a year. The AML/CFT issues are part of the obligatory post-recruitment tutoring kit and, subsequently, the employees take part in annual trainings and workshops organised by the AML/CFT Compliance team. Special courses for board members are also arranged. The quality and the content of the trainings are examined by the supervisors. The Compliance Officers of investment companies participate in 2-3 AML/CFT trainings per year. The FAU identified one breach related to the training obligations of a casino and applied a sanction, which demonstrate that in general the training obligations in casinos are observed. Both the FAU and the representatives of the casinos confirmed that the written AML/CFT procedures must be adopted and sent to the FAU for verification.

390. Many of the interviewed banks have, through internal procedures, a prerequisite of minimum 5 years of experience in financial crime, university degree and experience in management to accede in a position of AML/CFT Compliance Manager. However, there is no legal requirement to designate the Chief AML/CFT Compliance Officer(s) at the management level and there are no particular qualification requirements prescribed in the law. Banks screen prospective Compliance Managers and verify their criminal backgrounds based on internal regulation. Boards of large banks approve appointment of compliance officers.

391. The Compliance Officers of investment companies participate in 2-3 AML/CFT trainings per year. FAU identified one breach related to the training obligations of a casino and applied a sanction.

392. According to the Czech legislation, AML/CFT systems in all credit institutions, life insurance companies and pension companies are subject of independent internal audits without any specification regarding the periodicity. The financial institutions include the AML/CFT issues into their internal audit plans on the basis of their own risk assessments. The on-site interviews confirmed that banks do perform internal audits to check compliance with the AML/CFT internal procedures.

393. AML/CFT Compliance Units of the large Czech financial institutions are adequately resourced and often operate as independent structures. They report directly to senior management and make independent decisions whether or not to file STRs. In smaller FIs and DNFBPs the compliance functions are performed by the general management and this is primarily due to the very limited number of employees (sometimes two-three) and reduced size of the respective entity. In case of single independent professionals (such as auditors, notaries and lawyers) the audit is ensured by the SROs who demonstrated a satisfactory level of awareness on AML/CFT matters.

394. While banks, large financial institutions and DNFBPs have adequate level of internal control procedures (in written form), DNFBPs and small financial institutions fall well short of the desirable standards in this regard as the AML/CFT compliance procedures are included in general company's regulations and the audits are performed by the manager where an independent audit function cannot be established due to the limited size of the entity and small number of employees. This appears to be commensurate with materiality and risk. The evaluation team did not identify any legal or regulatory requirements impeding implementation of the Core Issue.

Conclusions

395. Banks, and to a large extent other large financial institutions, have a good understanding of their ML/FT risks and obligations. The on-site interviews revealed that the understanding of AML/CFT risks amongst the currency exchange sector and DNFBPs varies, and rarely involve risk-based approach to their AML/CFT measures.

396. Banks analyse their operation based on products/customers/transactions/location and classify as low/moderate/high risks, using advanced software tools and guidance from the European parent companies. The applied risk mitigating measures appear to be adequate. DNFBPs apply the risk mitigating measures commensurate to their limited understanding of AML/CFT risks.

397. The banks appear to be familiar with CDD obligations. CDD and on-going monitoring measures employed by DNFBPs are often fragmented, and do not imply risk-based approach.

398. The application of EDD measures - including EDD measures for PEPs - is not a requirement under the AML/CFT Law as such, which negatively impacts the application of the EDD measures by the private sector.

399. The Czech banks are the main contributors in terms of STR submission to the FAU while the volume of STRs submitted by non-bank financial institutions and DNFBPs is commensurate with their awareness in the ML/FT area. **The Czech Republic has a moderate level of effectiveness for IO.4.**

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

- The CNB has a robust FIs licensing mechanism, including a sound process to make sure that criminals are not owners or managers of financial institution. Some deficiencies have been identified in relation to the ability to recognize PEPs and associates of criminals in the authorisation process. For tight agents, the CNB relies on criminal records checks performed by the represented entity.

- The real estate agents, accountants, trust and company service providers, dealers in precious metals and stones and traders in items of cultural heritage or items of cultural value, are not subject to licencing and hence, no measures are in place to prevent criminals and their associates from being professionally accredited or holding a significant or controlling interest, or a management function in those DNFBPs.

- On AML/CFT supervision, the FIU and CNB are the two main regulators that simultaneously oversee the biggest part of Czech Republic's financial sector. The power of both institutions in terms of running on-site and off-site inspections and on imposing sanctions is very similar and applicable to the same categories of financial institutions. The efficiency of the existing model (duplication of duties for on-site AML/CFT supervision) might be an issue in a view of limited resources.

- The FAU and CNB have a good understanding of ML/FT risks in Czech Republic, this being facilitated by the fact that they are the drafter and the key contributor to the NRA report. The two main supervisors demonstrated significant efforts in promoting the results of the risk assessment amongst the entities under their remit and in promoting a clear understanding of AML/CTF obligations and ML/FT risks.

- CNB`s Financial Market Supervision Department has applied the most comprehensive AML/CFT risk-based supervision system (RAS/RAS II system). The models used by the FAU and CNB Financial Market Supervision Department II would benefit from being further developed to be more AML/CFT risk-based. The criteria used by professional Chambers for inspections planning do not contain specific ML/FT components.

- Starting 1 January 2017 the CNB was given the power to apply pecuniary sanctions for AML/CFT breaches based directly on the AML Act. This is a positive regulatory change aimed to improve the efficiency of AML/CFT supervisory measures, but not yet intensively used by the CNB. The fines applied by the FAU and CNB are not playing their dissuasive and deterrent role and they are not applied in a proportionate manner. No sanctions have been applied to natural persons. The level of sanctions that can be applied according to AML/CFT Law is low.

- The level of supervision of DNFBP sector has improved since the previous evaluation. The awareness and understanding of the supervisors of lawyers, notaries, auditors, bailiffs and tax advisors (professional Chambers) is at a satisfactory level. By the time of the on-site visit, only Czech Bar Association and Chamber of Notaries was able to demonstrate the application of a rather limited number of specific AML/CFT sanctions. No sanctions for AML/CFT breaches have been imposed by the others Professional Chambers.

- In a view of limited FAU and CNB Financial Market Supervision Department II resources for on-site supervision, the number of performed audits is low, especially in case of financial sectors

with high number of obliged entities (e.g. insurance intermediaries, non-banking payment services providers or electronic money issuers…). Therefore, the supervisory actions have a narrow impact on compliance. Supervision of DNFBPs is not at the stage where it can prove that it makes a difference to AML/CFT compliance.

Recommended Actions

The authorities should:

- enhance the licensing procedures for financial institutions and DNFBPs to include processes of verification of legitimate source of funds, in order to prevent integration of domestic and foreign criminal assets into the Czech financial system;
- take measures to prevent criminals and their associates from being professionally accredited or holding a significant or controlling interest, or a management function in all DNFBPs;
- take measures to ensure that their managers, UBOs or controllers are not the associates of criminals, including by using trustful international data bases.

The existing approach to supervision should be revised to:

- increase budgets and the number of staff for all AML/CFT supervisory authorities;
- place more focus on the risks connected with foreign incoming and out-going flows to prevent financial institutions and DNFBPs to act as intermediaries for the integration of foreign criminal assets into the Czech financial system;
- place more focus on the risks and vulnerabilities connected to the potential misuse of the financial system by fictitious entrepreneurships for ML/FT purposes;
- review the efficiency of the existing model which provides for significant duplication of duties for on-site AML/CFT supervision between regulators;
- review the supervision system by the DNFBPs supervisors and CNB Department II to be more AML/CFT driven;
- enhance FAU's risk-based approach to supervision;

With regard to sanctions the authorities should:

- apply dissuasive and proportional pecuniary sanctions to financial institutions and DNFBPs;
- clearly identify, for each sector, the management positions that can be sanctioned for AML/CFT breaches.

In addition to the above, the authorities should:

- amend the legislative framework to increase the level of sanctions to make them more proportionate and dissuasive;
- require credit institutions to have compliance programs providing for a designated AML/CFT Chief Compliance Officer(s) at the management level;
- introduce qualification requirements and "fit and proper tests" for AML/CFT Chief Compliance Officers.
- address the technical deficiencies identified in relation to R. 26 to 28 and 35.

Immediate Outcome 3 (Supervision)

400. According to Section 35 of the AML Act, the FAU has a general authorisation to supervise all financial institution and the DNFBPs other than legal and advisory professions[55]. The CNB supervises the banking sector, the capital market, the insurance industry, pension funds, credit unions, bureaux-de-change, payment system institutions, e-money institutions and non-banking consumer loan providers. Before the amendments to the AML Act were enacted in 2017, only the FAU had competences to conduct administrative proceedings concerning AML/CFT breaches. The CNB and other supervisory authorities obtained such competences only recently. The power of FAU and CNB in terms of conducting on-site and off-site inspections and on imposing sanctions is very similar and applicable to the same categories of financial institutions. There is on-going coordination of planning AML/CFT supervision as well as the practice of conducting joint inspections (see IO1). Nonetheless, seeing the limited resources, there is a question whether such approach is efficient and whether such duplication of duties can be reasonably justified.

Table 14: Structure of FIs and DNFBPs in the Czech Republic

Financial Institutions		
Sector	**No. of Registered Institutions**	**Value of assets (EURO[56])**
Banks and cooperative savings	58	265,6 bn
Life insurance companies	20	18,02 bn[57]
Insurance intermediaries	154 355	N/A
Non-bank payment service providers or electronic money issuers	209	2 600 349 000
Agents of Foreign payment institutions from MS		
Securities – investment firms	66	953 647 833
Investment companies	27	14 785 342 000
Self-governing investment funds	29	2 075 925 000
Non-bank foreign exchange entities	1 004	N/A
Pawnshops		
Lenders and credit intermediaries other than banks and savings banks		
Pension companies	8	17,0 bn
Leasing companies		

Type of business	**Supervisor**	**No. of Registered Institutions**
Casinos (which also includes internet casinos)	Customs Administration, Financial Analytical Office	263

[55] Accountants are supervised by the FAU although they are a part of legal and advisory professions.
[56] Exchange rate as of June 30, 2017
[57] According the Czech Generally Accepted Accounting Principles

Real estate agents	Trade Licence Office, Financial Analytical Office	N/A
Dealers in precious metals and precious stones	Trade Licence Office, Financial Analytical Office	N/A
Dealers in precious stones	Trade Licence Office, Financial Analytical Office	N/A
Lawyers, notaries, other independent legal professionals and accountants	Czech Bar Association, Chamber of Notaries, Chamber of Auditors, Chamber of Tax Advisors, Chamber of Bailiffs, Ministry of Finance	12901 (Lawyers), 449 (Notaries), 4703 (Tax Advisors), 154 (Bailiffs), 1598 (Auditors), N/A (Accountants)
Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere	Trade Licence Office, Financial Analytical Office	406

Licensing, registration and controls preventing criminals and associates from entering the market

The Czech National Bank (CNB)

401. As the financial market supervisory authority, the CNB issues authorisations (licenses) to the majority of entities providing services on the financial market. It also issues permissions, approvals or prior consents. Banks, credit unions, investment firms and intermediaries, accredited persons on the capital market, insurers and re-insurers, fund management and administration companies, pension management companies and accredited persons, payment institutions, electronic money institutions and small e-money issuers, credit consumer providers and accredited persons, and bureaux de change are licenced by the CNB.

402. The CNB has a separate Licensing Department which reviews the competence, trustworthiness and experience of the management of FIs (members of the statutory body, members of the administrative board and members of the supervisory board), and persons having a "qualifying holding". CNB conducts the "fit and proper tests" in compliance with the legislative requirements.

403. The procedures for submitting applications for permission or approval to the CNB are governed by the relevant sector-specific laws and subsequent decrees issued by the CNB. These regulations provide the specific requisites of applications, the specimen forms for applications, and the annexes that must be attached.

404. Banks, and other licensed financial institutions[58] are required to notify the CNB of proposed personnel changes in the statutory body, the administrative board and the supervisory board, and submit the necessary documents evaluating their competence, trustworthiness and experience. Every candidate for Board of Directors and Supervisory Board of a bank is subject to a "fit and proper" test. The information submitted by the candidate is analysed to verify the clean criminal record, professional experience and the strategy proposed for the new function. In the verification process, all CNB departments that may have any information on the person under scrutiny are asked to deliver comments or information detained. In case the candidate is a foreigner or was active abroad, the CNB contacts the relevant foreign supervisors and seek their input.

[58] credit unions, insurance companies and pension funds, investment firms, management companies, non-bank consumer credit providers, non-bank payment service providers, electronic money issuers, investment intermediaries, consumer credit intermediaries, non-bank foreign exchange entities

405. The CNB`s Interviewing Committee[59] (which includes representatives of supervision departments), considers the candidate and makes a recommendation for further decision. If needed, the Committee can meet and interview the candidate. The final approval is given by the head of the Financial Market Supervision Department. For all FIs (with the exception of tight agents) a prior consent of the CNB is required for Directors to start performing their functions.

406. If any shortcomings are identified in the activities of an entity, the CNB may require the replacement of a member of the statutory body, of the administrative board or of the supervisory board, a senior officer or any other responsible person.

Case example – withdrawal of an approval for an managing person.

The approval of a managing person of an investment fund granted to Mr. L was withdrawn by the decision of the CNB of 13 February 2017. In 2015, Mr. L. had been a managing person of investment fund A during the period in which the company had committed an administrative offence by unlawfully performing an activity without the licence. The company was punished by the penalty of 2 500 000 CZK (EUR 96,953) by the decision of the CNB.

Mr. L had also been a managing person of an investment fund B during the period in which this company had committed an administrative offence consisting in offering investment securities to the public without priory publishing the prospectus approved by the CNB. In 2015, the company was sanctioned with a 650 000 CZK (EUR 25,207) fine by the decision of the CNB. CNB conclusion was that Mr. L. had been a managing person of companies which had committed serious infringements of legal regulations, and therefore **he lost one of the preconditions necessary for discharge of the function of a managing person –trustworthiness.**

407. Significant changes in ownership structure of FIs are subject to the CNB approval. A prior consent of the CNB is necessary for a person to acquire a qualifying holding, or to increase the qualifying holding in a financial institution to 20%, 30% or 50%, or to become a person controlling a financial institution. The approvals are following the standard licensing procedure, with a focus on the source of funds (this is considered to be the "first firewall" in the licencing process).

408. To ensure that criminals are not owners or managers of financial institution, the CNB verifies all relevant persons concerned, by performing checks on the criminal record database to which it has direct access. In case of foreigners, it requires copies of the excerpts from their criminal records from the country of origin. Other sources, such as the insolvency register and CNB`s own database on the sanctions imposed are consulted. However, little is done to check that relevant individuals are not associates of criminals. No international data bases are available to the CNB.

409. No person has been rejected so far in the licencing process, but according to the CNB in the last 10 years there have been 5 examples of applicants withdrawing their applications prior to a potential negative decision from the CNB. No further measures have been taken in those cases.

410. The CNB recalls only one case when a PEP was identified as owner or manager of a financial institution but in the view of the evaluation team, little has been done to achieve effective screening of PEPs and apply subsequent risk mitigation measures.

411. For some categories of entities which are subject to registration, the CNB is relying on criminal records checks performed by the represented entity.

[59] The Interviewing Committee was established by the decision of the Director of the Financial Market Supervision Department I as an advisory body to the Director of that/this Department.

412. The 2012 "Czech Republic Financial Sector Assessment Program Documentation on Detailed Assessment of Observance of Basel Core Principles for Effective Banking Supervision"[60], included important recommendations, *inter alia*, "to require credit institutions to have compliance programs, with components for audit, training, and a designated compliance officer(s) at the management level, that address AML/CFT and financial crime". The second part of the recommendation was not implemented at the time of onsite visit, meaning that the AML/CFT Chief Compliance Officers of credit institutions were not subject to any mandatory qualification requirements or "fit and proper tests". CNB advised that the level of proficiency of AML/CFT compliance positions is checked within the course of the inspections. However, the absence of a mandatory requirement significantly limits CNB`s ability to apply "fit and proper" tests for Chief AML/CFT Compliance Officers, to make a decision on eventual professional incompatibilities, and to demand the dismissal of the person from position in case of significant AML/CFT violations. The evaluation team was advised that some of the management positions in financial institutions are subject to "fit and proper" tests but the list of such management positions was not available.

Gambling

413. For the Gambling sector, the licensing process is divided between the Ministry of Finance (that issues basic licences) and the municipal authority (that issues the licences for the gambling premises). The basic license must be obtained before the actual gambling activities start. The basic licencing process includes the analysis of the status of the operator (criminal record, solvency) and the compliance with the technical requirements.

414. The licensing procedure requires each operator to present a number of documents proving economic stability, transparent ownership structure, the origin of assets and good reputation of management. According to the information provided by Ministry of Finance, in the licensing process (which takes several months), the applicant itself has to prove a clean criminal record, legitimate source of funds and the adoption of AML/CFT internal regulations. Subsequently, the Ministry of Finance verifies the provided data using publicly available sources. A special focus is placed on the understanding of the ownership structure of the company. It was not clear for the evaluation team how the source of funds is verified and how a possible association with a criminal is prevented. No licencing applications have been rejected by the Ministry of Finance so far. Verbally it was confirmed that there have been cases of application withdrawn but no statistics have been provided.

Professional chambers - Czech Bar Association, Chamber of Tax Advisers, Notarial Chamber, Bailiff Chamber, Chamber of Auditors

Notaries

415. Notaries are organised in eight regional Notarial Chambers spread throughout the territory of the Czech Republic. Notaries are appointed by the Ministry of Justice and, during the accreditation process, a competition must be passed. As a part of the accreditation procedure, the candidate must prove a clean criminal record and pass a personal interview with a specialised Commission of the MoJ. Once a person becomes a notary, on-going controls of professionalism and good reputation are performed by the Notarial Chambers.

[60] https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/en/about_cnb/international_relations/imf_wb/download/fsap_cr_fsap_basel_core_principles.pdf)

Bailiffs

416. Judicial officers (bailiffs) carry out compulsory enforcement of enforcement titles (e.g. enforceable decision of a court, enforceable arbitral award, notarial record with permission for enforcement, enforceable decision of a public administration body) and other specific activities[61]. As of July 2017 there were 152 judicial officers in the Czech Republic. A clean criminal record is one of mandatory criteria for each person applying for bailiff license. The Minister shall remove the bailiff if he/she was sentenced upon the final and conclusive judgment for a malicious crime or for a crime committed in connection with the bailiff's activity. Every newly appointed Bailiff is checked by the Chamber on the first year of activity and then based on random checks.

Auditors

417. Auditors are obliged to follow the International Standards on Auditing (ISAs), specifically ISA 240[62]. To be registered in the Chamber of Auditors, the candidate needs to prove a clean criminal record and good reputation. In case a criminal investigation is commenced in relation to an auditor, he/she is suspended by the Chamber whilst in case of a conviction the auditor is de-registered. The representatives of the Chamber of Auditors informed the assessment team that approximately 15-50 disciplinary measures for misdemeanours were taken annually.

Tax Advisors

418. The Chamber of the Tax Advisers of the Czech Republic associates over 4 700 tax advisors – natural persons – and 980 legal persons providing tax advisory services. One of the conditions for becoming a member of the Chamber and therefore provide tax advisory services, is to have a clean criminal record. If a registered tax advisor is subject to prosecution he/she is obliged to notify the Chamber about this circumstance. The Chamber has the capacity to suspend or expel a member in case of a criminal conviction.

Lawyers

419. To be registered in the Czech Bar Association a candidate lawyer must provide a clean criminal record. The same applies to those lawyers who practice law in specialised firms: they all have to be registered by the Bar Association. In case a law firm is bought by a person who does not fulfil the conditions for practicing the legal profession, or in case a non-lawyer becomes a representative of a law firm, such entity loses the authorisation to provide legal services and is then excluded from the Register of Lawyers.

420. In case of an investigation against a lawyer, he/she needs to inform the Bar immediately. Until the investigation is completed, the licence is suspended and the person cannot act as a lawyer. Overall, "fit and proper" regime for notaries, bailiffs, auditors, tax advisors and lawyers, put in place by their professional chambers, is effective and prevents criminals from entering those DNFBPs sectors.

[61] Provide a legal aid; take into custody money, documents and other movables; deliver documents; carry out an auction of a movable or immovable property on the proposal of the owner or a person authorised to dispose of the property; ascertain property subject to seizure under a decision issued in a criminal proceeding; draws up executorial records etc…

[62] The Auditor´s Responsibilities Relating to Fraud in an Audit of Financial Statements

Other DNFBPs

421. The real estate agents, accountants, trust and company service providers and dealers in precious metals and stones and traders in items of cultural heritage or items of cultural value, are not subject to licencing and hence, no measures are in place to prevent criminals and their associates from being professionally accredited or holding a significant or controlling interest, or a management function in those DNFBPs. Only the TCSPs are registered (see Table 14).

Supervisors' understanding and identification of ML/TF risks

Financial Analytical Office (FAU)

422. The general ML/FT risks in the financial and other supervised sectors are well understood by the FAU. This is facilitated by the fact that the FAU was the coordinator and the main drafter of the Czech Republic NRA report.

423. FAU's Supervision Division cooperates with other supervisors and seeks input from the FAU`s analytical department to widen its understanding of risks. The authorities advised that an important instrument in evaluating the risks and is the review of the AML/CFT internal procedures of the reporting entities.

424. To extend its understanding of ML/FT risks and to identify new risks, the FAU uses information from the CNB inspections, from other supervisors, police, private persons and from STRs.

The Czech National Bank (CNB)

425. The CNB actively participated on the preparation of the NRA by feeding in information on results of its supervisory activities, and by providing comments to the document as a whole. In general, the CNB has a good understanding of ML/FT risks. Financial institutions (except for currency exchange offices and the non-banking payment service providers) must send up-to-date internal AML/CFT rules and risk assessments to the CNB. Based on those evaluations, the CNB identifies current ML/FT trends and risks and uses the results to target areas of focus in its supervisory actions. The CNB closely co-operates with the FAU and foreign supervisory authorities.

426. To understand ML/FT risks and to identify new risks, CNB uses information obtained from on-site or off-site supervision tools which are closely related. Given continuous access to an extensive set of information, CNB systematically identifies potential risks (in both prudential and AML/CFT supervision), assesses such risks and proposes necessary remediation measures.

Supervisors of DNFBPs - Czech Bar Association, Chamber of Tax Advisers, Notarial Chamber, Bailiff Chamber, Chamber of Auditors

427. The representatives of the management of professional Chambers demonstrated a relatively good level of understanding of AML/CFT obligations as well as awareness of the NRA results. To obtain information on AML/CFT risks, the Chambers use different information sources including previous audits results, negative information from media, complaints, verification of new members, verifications of members before exiting the profession etc.

428. The Customs Administration is the new supervisor for the gambling business since 2017. The Customs Administration has a basic understanding of ML/FT risks as it has only started performing these functions.

429. According to the authorities, the Czech Trade Inspection carries out inspections according to the powers defined by AML/CFT Act, but no information on Czech Trade Inspection understanding and identification of ML/FT risks was available for the assessment team.

Risk-based supervision of compliance with AML/CTF requirements

The Czech National Bank (CNB)

430. At the decision of the Bank Board, the CNB's supervisory work was re-organised as of 1 March 2017. Supervision is currently performed by the Financial Market Supervision Department and the Financial Market Supervision Department II. The difference between Financial Market Supervision Department and the Financial Market Supervision Department II is in the type of FIs they are in charge of. The authorities explained on-site that this set-up was put in place with the view to enable the supervisors to focus constantly on entities engaged in the distribution of financial products and bureau-de-change activities, and to allocate sufficient supervisory capacity to all entities. The change was also due to the CNB's new supervisory competences on intermediation of consumer credit.

CNB`s Financial Market Supervision Department

431. The Financial Market Supervision Department conducts off-site and on-site supervision of: credit institutions; insurance and reinsurance corporations and pension funds. In all their supervisory activity, the CNB applies a risk-based approach using an internal analytical tool (Risk Assessment System – RAS) that combines the results of both off-site analyses and on-site examinations.

432. The complexity of RAS rating depends on the relative importance of the subsector within the whole financial area. The most complex rating is designed for banks and insurance companies. The rating is re-assigned semi-annually (for banks and insurance companies) and annually for smaller/less important entities. RAS is used to calculate Prudential Rating (PR), Conduct of Business Rating (CBR) and Anti-Money Laundering Rating (AMLR).

433. For AML/CFT rating of financial institutions RAS uses the following qualitative criteria: (i) customers identification process, (ii) KYC and customer´s categorization, (iii) record keeping, (iv) AML/CFT internal rules, (v) the process of suspicious transactions detection and reporting to FAU, (vi) mechanisms of internal AML/CFT controls and (vii) the AML/CFT training. The individual AML/CFT risk profile based on above mentioned criteria has been complemented by manually-considered criteria which include: period from the last AML/CFT on-site inspection, seriousness of deficiencies identified during the last AML/CFT on-site inspection, fulfilment of imposed remedial measures according to schedule and in desired quality, significance of the institution in the financial market, sectorial risk, and information received from other CNB´s departments, FAU, foreign regulators or as identified in the media.

434. In 2018 the Financial Market Supervision Department I compiled an annual AML/CFT on-site inspection plan based on a risk assessment pilot-project for banks and credit unions, using three main information sources: AML/CFT screening (self-assessment questionnaire), results from previous AML/CFT on-site inspections and on-going off-site monitoring.

435. As a result of the application of the pilot project, the individual risk profile of the concerned financial institution was determined. CNB Financial Market Supervision Department plans to amend the individual risk profile of the supervised institution on annual basis, and adjust the risk assessment methodology. In a view of the assessment team, the Financial Market Supervision Department has applied a comprehensive risk-based supervision system, which can produce adequate rating of different FIs based on their AML/CFT risks.

CNB`s Financial Market Supervision Department II

436. The Financial Market Supervision Department II conducts off-site and on-site supervision of:

- electronic money institutions, foreign electronic money institutions operating in the Czech Republic through a branch,
- payment institutions, foreign payment institutions operating in the Czech Republic through a branch,
- small-scale electronic money issuers,
- small-scale payment service providers,
- investment intermediaries and their tied agents,
- insurance intermediaries and independent loss adjusters,
- bureaux de change,
- non-bank investment firms and their tied agents,
- management companies,
- autonomous investment funds,
- depositaries and administrators of investment funds, except in the case of banks,
- entities authorised to provide or intermediate consumer credit if subject to CNB supervision,
- accredited entities in accordance with the sectorial legislation (hereinafter referred to as "supervised entities").

437. When evaluating the risk profile of entities under its supervision, the CNB Financial Market Supervision Department II takes into account the NRA, and in most cases the AML/CFT supervision is combined with prudential supervision. The Financial Market Supervision Department II divided the supervised entities into 3 categories (A, B, C). Category A contains high-risk entities with a significant market share and vast territorial scope. The periodicity of on-site inspection is based on the risk profile of specific segment of financial market into which the supervised entity belongs, on the risk profile of specific supervised entity and on the off-site supervisory information.

438. In case of non-banking payment service providers, the periodicity of on-site inspections for category A entities is generally set at 4 years, for category B at 7 years. For category C, on-site inspections are conducted only based on a prior warning (complaints, negative media reports etc…). The classification is reviewed annually. Substantial changes in the management or in the business activities may constitute grounds for a risk profile update and an ad hoc inspection can be initiated.

439. Although essentially risk based, the model for determining the frequency and intensity of on-site supervision used by the CNB Financial Market Supervision Department II would benefit from being more AML/CFT driven.

440. The number of audits performed for banks and non-bank foreign exchange entities appears to be sufficient and efficiently risk based. On a less positive note, the number of audits performed for some of the non-banking financial institutions[63] is not satisfactory and, in the assessors' opinion, is due to lack human resources.

[63] Investment firms, Investment intermediaries, Investment funds, Insurance companies and insurance intermediaries, , Non-banking payment services providers or electronic money issuers or providers of small extent payment services, Independent customer credit intermediaries and Tied agents of customer credit according to the Consumer Credit Act

Table 15: AML/FT on-site inspections conducted by CNB and FAU in financial institutions

Years	Total number of entities	Number of AML/CFT specific on-site visits conducted	Number of AML/CFT combined with general supervision on-site visit carried out
Banks and cooperative savings			
2012	56	CNB 10 FAU 1	
2013	58	CNB 10 FAU 3	
2014	56	CNB 8 FAU 4	
2015	57	CNB 10 FAU 4	
2016	56	CNB 12 FAU 3	
- June 2017	56	CNB 4 FAU 1	
Securities – Investment firms			
2012	61	2	
2013	64	2	
2014	58	3	
2015	62	CNB 6 FAU 2	
2016	65	CNB 4 FAU 1	
- June 2017	66		
Investment intermediaries			
- June 2017	7296		4
Management companies			
2012	21	3	
2013	24	2	
2014	26	CNB 2 FAU 1	
2015	29	2	
2016	28	4	
- June 2017	27		
Self-managed investment funds			
2012	77	2	
2013	13	1	
2014	17	4	
2015	29		
2016	27		
- June 2017	29		
Pension funds			
2012	9		
2013	10		
2014	9		
2015	8	1	
2016	8	1	
- June 2017	8		
Life insurance companies + insurance intermediaries			
2012	130 001 (21+129 980)		66
2013	137 697 (20+137 677)		76
2014	143 758 (21+143 737)	2	70
2015	148 550 (21+148 529)	2	42
2016	152 759 (20+152 739)	1 + 0	0 + 35
June 2017	154 375 (20+154 355)	1 + 0	0 + 5
Non-bank foreign exchange entities			
2012	933	FAU 3	CNB 129
2013	960		134
2014	970	FAU 5	CNB 66

2015	**984**	**CNB 2 FAU 32**	**CNB 43**
2016	**987**	**FAU 41**	**CNB 47**
- June 2017	**1 004**	**FAU 11**	**CNB 19**
Non-banking payment services providers or electronic money issuers or providers of small extent payment services			
2012	**85**	**FAU 1**	**CNB 16**
2013	**99**	**FAU 7**	**CNB 11 FAU 7**
2014	**124**	**FAU 8**	**CNB 7**
2015	**156**	**CNB 40 FAU 3**	**CNB 11**
2016	**185**	**FAU 5**	**CNB 12**
- June 2017	**209**	**FAU 1**	**CNB 2**
Independent customer credit intermediaries			
- June 2017	**167**		
Tied agents of customer credit according to the Consumer Credit Act			
2016	**3505**	**FAU 1**	
- June 2017	**23 902**	**FAU 1**	

441. As described above, there are significant differences in the risk assessment models and the ways of AML/CFT supervision is conducted by the two CNB Departments. The authorities explain this by different size and level of AML/CFT risks represented by different supervised sectors. Financial Market Supervision Department has staff entirely responsible for conducting on-site AML/CFT audits and has a comprehensive risk-based supervision system. The Financial Market Supervision Department II conducts AML/CFT supervision combined with prudential supervision and consumer protection supervision.

Financial Analytical Office (FAU)

442. With limited human resources, (5 employees responsible for AML/CFT supervision of all obliged entities) the FAU performs inspections only of the reporting entities with high ML/FT risks. The planning of inspection is primarily based on the NRA, analysis of the internal systems of rules, publicly available sources, inspections carried out in the past (both by the FAU and the CNB) as well as the information obtained from the FAU analytical department.

443. The inspection plan is completed at the beginning of every year but can be and is continuously updated following any changes in the risk assessment of supervised sectors or the obliged entities. Depending on the identified ML/FT risks, the area of supervision and the amount of required documents related to the inspection may be widened or narrowed.

444. For the exchange bureaux, the FAU has the ability to perform the so called "control purchases". This tool has been in use since 2014 and consists in anonymous visits to currency exchangers demanding the conversion of a sum above the identification threshold (EUR 1,000). In the event the operation is executed without identification, an inspection report is drawn, the obliged entity is fined and corrective actions are imposed to ensure compliance.

445. There is a strong cooperation between the FAU and other supervisors on ML/FT issues which includes information exchange on inspections results, joint AML/CFT audits (CNB) and coordination of AML/CFT on-site planning. Coordination of AML/CFT on-site planning is performed to ensure that same FIs are not audited twice by different regulators. As mentioned under IO1, in 2015 and 2017 the CNB and the FAU carried out joint AML/CFT on-site inspections in two financial institutions. As highlighted above, there is a question whether existing approach is efficient and whether such duplication of duties of FAU and CNB can be reasonably justified.

Supervisors of DNFBPs - Czech Bar Association, Chamber of Tax Advisers, Notarial Chamber, Bailiff Chamber, Chamber of Auditors

446. The Chambers regularly perform different controls over the activity of their members. The AML/CFT supervision is a part of the general (prudential, regulatory) controlling actions. For the purpose of planning the audits, the Chambers apply different general and professional criteria including previous audits timeframe, previous audit results, negative information from media, complaints, verification of new members, verifications of members before exiting the profession, etc. However, the criteria used by the Chambers for inspections planning (which is essentially risk-based) do not contain some specific ML/FT components. While understanding that a pure AML/CFT supervision with a stand-alone AML/CFT risk assessment model for professional chambers might not be the ideal setting, ML/FT risks and elements should be included in the overall criteria used for organising the supervisory actions.

Other DNFBPs supervisors

447. The Czech Customs Administration, the new supervisor for gambling business since 2017, conducts combined inspections that include ML/FT issues but does not apply a risk based approach. According to the authorities, the Czech Trade Inspection carries out inspections according to the powers defined by AML/CFT Act but no information on the AML/CFT supervisory activity was provided.

Remedial actions and effective, proportionate, and dissuasive sanctions

448. The range of fines that can be applied for failure to comply with the obligations stipulated by the AML/CFT law is indicated in section 35.1 of TA. The maximum level of sanctions provided by AML/CFT Law is up to CZK 10,000,000 (~ EUR 370,500).

Financial Analytical Office (FAU)

449. In the course of 2017, due to changes in AML/CFT Law which added an obligation to draw up written risk assessments and broadened the scope of obliged entities (e.g. all operators of gambling instead of only operators of live games, investment intermediaries and entities dealing with virtual currencies), there was a significant increase in the number of AML/CFT internal rules and procedures delivered to the FAU. The authorities advised that the internal rules often contain a number of shortcomings (the highest quality lays with the banks, credit unions, insurance companies and electronic money institutions), one of the most common being the lack of implementation of a full risk based approach.

450. Due to a large number of deficiencies, the revision of the internal rules is a long process which requires repetitive written notification the obliged entity. This system appears to be time-consuming for the supervisors, and bearing little efficiency. The existing framework would benefit if the attention of the supervisors would be shifted from reviewing the internal rules, to verification of the implementation of the AML/CFT system through on-site/off-site inspections.

451. The most frequent violations detected by the FAU within the framework of the on-site inspections are weaknesses in the field of identification of the client, and lack of proper CDD. In case deficiencies are identified, the obliged entity must draw up a report on corrective actions and submit it to the FAU within a certain deadline. The FAU monitors the implementation of the corrective actions. In case the obliged entity does not elaborate the report, a fine of up to CZK 500,000 (EUR 19,000) may be imposed under the Control Code. In practice, this power has been used several times.

452. If the control findings are serious and are not adequately remedied, the FAU can initiate a misdemeanour proceeding under which a fine of up to CZK 1-10 million (EUR 39,000 – 390,000) can be imposed, doubled by the publication of the decision on the FAU's website for a period of 5 years. The later has never been used in practice due to recent adoption of the provision and lengthy administrative procedures in case of litigation.

453. If the obliged entity committed a breach of its obligations repeatedly or in particularly serious circumstances, pursuant to Section 36 AML Act, the FAU can submit an initiative to revoke or withdraw its license to the institution which granted it. Although this power was used several times and initiatives were sent to the CNB (with regard to an exchange offices), no licence was withdrawn so far.

454. The lowest fines amount to around CZK 20,000 (EUR 800) and were imposed by the FAU in the context of the "controlled purchases". The highest fine was imposed by the FAU in 2013 in the amount of CZK 2.5 mil (EUR 96.000) for non-implementation of the CDD and failure to submit STR by a payment institution. The second highest fine was imposed by the FAU in 2016 in the amount of CZK 1 mil. (EUR 39,000) to a bank for failure to perform identification of the customer.

FAU supervision – case

In the course of its supervisory actions, the FAU identified a payment service provider who repeatedly failed to correctly apply the CDD measures and to report suspicious transactions. Further analysis of the company's records demonstrated a systemic error which led to defects in obtaining the compulsory information regarding the purpose and intended nature and the source of the funds used. The misconduct involved large volume of funds originating from abroad.

Consequently, using the "absorption principle" (the fine was imposed for the most severe misconduct) a fine of 96.000 EUR has been imposed. When assessing the amount of the fine, the FAU took into consideration the company's profit, the seriousness of the offence, and the volume of the funds involved. Subsequently the company filed a suit against the Ministry of Finance asking for the annulment of the fine. The Municipal Court in Prague dismissed the action in January 2018 as unfounded.

Table 16: Total volume of AML/CFT sanctions or other measures imposed by Czech Republic supervisory authorities from January 2012 until June 2017

Year	Number of inspections having identified AML/CFT infringements	Type of sanction/measure applied				
		Written warning	Fines		Removal of manager/ compliance officer	Withdrawal of license
			Number	Amount (EUR[64])		
2012	152	109	11	32 061		
2013	142	87	17	124 160		
2014	98	27	18	69 274		
2015	104	25	34	133		

[64] 1 EUR = 26,2 CZK

				345		
2016	**80**	**30**	**15**	**98 665**		**1**[65]
June 2017	**31**	**23**	**12**	**27 099**		
Total	607	283	95	484 604		

455. The level of available sanctions in the Czech Republic is low, but even so, the maximum sanction (CZK 10 million/EUR 390,000) has never been applied. The total fines to all obliged entities in the country never exceeded EUR 140,000. Seeing the size of the financial sector and the DNFBPs in the Czech Republic, in conjunction with the country AML/CFT risks, the assessment team concludes that AML/CFT sanctions applied so far are not dissuasive and proportional. Certain sanctions (e.g. removal of a manager) have not been imposed so far, and no fines or other sanctions have been imposed to individuals. There was one case of license revocation of a local bank in 2016 (see details in the Case Example below), the main breaches identified were of prudential nature (malfunction of bank's governance systems and exceeding the limits to large exposures) with some AML/CFT component.

The Czech National Bank (CNB)

456. As a general approach for CNB inspections, the supervised entity is invited to submit remedial measures to address the shortcomings identified or the administrative procedure is initiated to impose a fine and/or remedial measure. In the financial sector in 2016 approximately half of the on-site inspections resulted in imposition of remedial measures.

CNB`s Financial Market Supervision Department

457. CNB`s Financial Market Supervision Department has six on-site inspectors entirely responsible for conducting on-site AML/CFT audits in 47 banks (including foreign bank branches), 10 credit unions, 20 life insurance companies and 8 pension companies (as of 30 June 2017).

458. The most common deficiencies identified by CNB`s Financial Market Supervision Department during AML/CFT on-site inspections relate to CDD performance. Following a supervisory action, when a breach is identified, the CNB first gives a written warning and an order for remedial actions. As a result, the reporting entity prepares an action plan with concrete steps and specific timelines for remediation measures, which is approved by the CNB. The report on the status of the implementation of the corrective measures is sent to the CNB usually on a quarterly basis. If the institution does not comply with the action plan, sanctions shall be applied.

459. The most severe sanction imposed by the CNB was in 2016 when the licence of a local bank was revoked. The main breaches identified were of prudential nature with some AML/CFT component.

CNB supervision case – withdrawal of the banking licence

In the course of its supervisory actions, the CNB noticed an unusual and unreasonable decline in liquid assets of bank's accounts on 19 – 20 September 2016 (CZK -153.700.000/EUR 5,900,000). CNB considered the situation serious enough to report it as a suspicious transaction to FAU on 7 October 2016. According to the AML Act, the CNB simultaneously suspended the execution of any transaction of the client by putting a hold on payments going out from bank's accounts kept in the CNB.

[65] The CNB revoked the licence of a local bank. The main reasons for this action were the bank's non-functioning governance system and purchases of bonds in contravention of legal rules and subsequently the deficiencies in the AML/CFT system.

On 10 October 2016, FAU lodged a criminal complaint to the Prosecuting Authorities based on the CNB's STR, and ordered the CNB to suspend the transactions for three more days. On 12 October 2016, the Police Authority with the previous consent of the Public Prosecutor adopted a resolution on freezing assets at bank's accounts up to CZK 1.400.000.000 (EUR 53.000.000).

The withdrawal of the bank's licence came into force on October 24, 2016. The reasons for the CNB's decision to withdraw the banking licence were malfunction of E-bank's governance systems and exceeding the limits to large exposures. On 24 October 2016, the Municipal Court in Prague adopted a resolution on winding up and liquidation of the bank and nomination of a liquidator. The resolution has been preliminary enforceable since 25 October 2016.

CNB`s Financial Market Supervision Department II

460. As in the case of Department I, an integral part of off-site supervision is the assessment of the AML/CFT internal procedures. The capital market companies (incl. 7,296 investment intermediaries) are obliged to submit to the CNB their AML/CFT internal rules (including written risk assessment) within 60 days of being granted a licence. Any change shall be notified within 30 days of the adoption. The CNB assesses the documents and in case of deficiencies, requests remedies to be applied. The respective obliged entity must subsequently inform the CNB about the implementation of remedial measures. The currency exchange offices and the non-banking payment service providers do not have a statutory obligation to submit to the CNB their internal rules. As described above, the Financial Market Supervision Department II doesn't have an AML/CFT dedicated Unit. The overall number of staff is 100 - they are in charge of all supervisory activities.

461. It is the assessors' view that such a system (mandated by Section 21/8 of AML Act) bares little effectiveness and the verification of whether the system of internal rules is functional or not can only be verified in the framework of AML/CFT inspections.

462. In the course of the on-site supervision, the most common AML/CFT deficiencies identified relate to: insufficient AML/CFT training provided to staff; self-evaluation reports (obligation stemming from the CNB Decree (Art. 8); internal procedures insufficiently developed; deficiencies in relation to individual transactions.

463. Based on the seriousness and nature (systemic or individual) of the deficiencies, the CNB`s Financial Market Supervision Department II can request corrective measures (written warning) or initiate administrative proceedings to impose a sanction (fine/withdrawal of the licence).

464. In case of a request for remedy, the supervised entities submit a follow-up list of implemented measures. If the remedial measures appear to be insufficient, the CNB`s Financial Market Supervision Department II can initiate a follow-up on-site inspection focused on detailed assessment of remedial measures.

465. In 2017 and 2018, the CNB started applying administrative proceedings for AML/CFT breaches but, as in the case of Department I, the sanctions do not appear to be proportionate, and only partially dissuasive taking into account the size of financial sector and the threats identified. Other sanctions have not been used and no fines or other sanctions have been imposed in relation to individuals.

Table 17: AML/CFT sanctions or other measures imposed by Financial Sector supervisory authorities

Year	Number of inspections	Type of sanction/measure applied			
		Written	Fines	Removal of	Withdrawal

	having identified AML/CFT infringements	warning	Number	Amount (EUR[66])	manager/ compliance officer	of license
Banks and cooperative savings						
2012	**11**	**9**	**2**	**5 724**		
2013	**11**	**10**				
2014	**9**	**8**	**1**	**5 725**		
2015	**16**	**9**	**5**	**41 985**		
2016	**14**	**12**	**2**	**43 893**		**1**[67]
June 2017	**4**	**4**				
Total	**65**	**52**	**10**	**97 327**		
Securities – Investment firms						
2012	**3**	**2**	**1**	**1 908**		
2013	**2**	**2**				
2014	**4**	**3**	**1**	**3 817**		
2015	**5**	**4**	**2**	**18 842**		
2016	**3**	**3**				
Total	**17**	**14**	**4**	**24 567**		
Investment intermediaries						
June 2017	**1**					
Total	**1**					
Management companies						
2012	**2**	**2**				
2013	**2**	**2**				
2014	**2**	**2**				
2015	**2**	**2**				
2016	**4**	**4**				
June 2017		**8**				
Total	**12**	**20**				
Self-managed investment funds						
2012	**2**	**2**				
2013	**1**	**1**				

[66] 1 EUR = 26,2 CZK

[67] The CNB revoked the licence of a local bank. The main reasons for this action were the bank's non-functioning governance system and purchases of bonds in contravention of legal rules and subsequently the deficiencies in the AML/CFT system.

2014	**6**	**4**	**2**	**5 725**		
June 2017		**10**				
Total	**9**	**17**	**2**	**5 725**		
Pension companies						
2015	**1**	**1**				
Total	**1**	**1**				
Life insurance companies + insurance intermediaries						
2012	**47**	**40**				
2013	**50**	**32**	**4**	**2 366**		
2014	**3 + 34**	**2+4**	**1**	**572**		
2015	**5 + 12**	**2 + 3**	**3**	**6 870**		
2016	**2 + 9**	**1 + 0**	**1**	**572**		
June 2017	**1+3**	**1+0**				
Total	**166**	**85**	**9**	**10380**		
Non-bank foreign exchange entities						
2012	**74**	**49**	**6**	**15 267**		
2013	**64**	**34**	**8**	**4 046**		
2014	**29**	**3**	**6**	**13 359**		
2015	**32**	**2**	**21**	**51 908**		
2016	**36**	**7**	**9**	**28 626**		
June 2017	**21**		**11**	**23 282**		
Total	**256**	**95**	**61**	**136 488**		
Person authorised to buy and trade in debts and receivables						
2013	**2**		**2**	**10 687**		
Total	**2**		**2**	**10 687**		
Non-banking payment services providers/electronic money issuers/providers of small extent payment services						
2012	**10**	**5**	**2**	**9 160**		
2013	**10**	**6**	**3**	**107 061**		
2014	**6**	**1**	**2**	**13 359**		
2015	**29**	**3**	**1**	**11 450**		
2016	**9**	**2**	**1**	**7 634**		
June 2017	**2**		**1**	**3 817**		
Total	**66**	**17**	**10**	**152 481**		

Supervisors of DNFBPs - Czech Bar Association, Chamber of Tax Advisers, Notarial Chamber, Bailiff Chamber, Chamber of Auditors

466. The AML/CFT responsibilities are relatively new for the professional chambers that otherwise have the experience, powers and ability to perform regularly supervisory actions. AML/CFT checks are performed in the context of the general audits (Chambers of Auditors mentioned BO and CDD related items) and in some cases have a AML/CFT risk based component (the Bar Association and the Chamber of Notaries are looking more closely to professionals who manage deposits on behalf of their clients and who hold escrow accounts). Initiating disciplinary proceedings for various breaches is not uncommon for the professional chambers (150 for the Bar Association, 15-50 per year for the Chamber of Auditors, 10 cases in the last year for the Chamber of Tax Advisors). At the time of the on-site visit, the Czech Bar Association informed the evaluation team that in 2017, out of a total of 37 disciplinary decisions, 10 were related to the AML/CFT breaches. The Notary Chamber also mentioned one sanction applied for AML/CFT violations. Other Professional Chambers did not impose specific sanctions. No information on sanctions imposed by Chambers was included in the NRA.

The Customs Administration

467. The Customs Administration, as a new supervisor for gambling business which started conducting inspections that include AML/CFT component since 2018, has not yet imposed any sanctions for AML/CFT breaches.

468. Inspections of casinos, real estate and trust and company service providers as indicated in the Table below were conducted by the FAU. The pecuniary sanctions do not appear to be proportionate and dissuasive. Other sanctions have not been used and no fines or other sanctions have been imposed in relation to individuals.

Table 18: AML/CFT sanctions or other measures imposed by DNFBP supervisory authorities

Year	Number of inspections having identified AML/CFT infringements	Type of sanction/measure applied				
		Written warning	Fines		Removal of manager/ compliance officer	Withdrawal of license
			Number	Amount (EUR)		
Casinos						
2014	**1**		**1**	**5 725**		
2016	**1**		**1**	**7 634**		
Total	**2**		**2**	**13 359**		
Real estate						
2014	**2**		**2**	**6 870**		
2015	**1**		**1**	**7 634**		
Total	**3**		**3**	**14 504**		
Dealers in precious metals and stones						
none						
Lawyers						
2017	**10**		**10**			**2**
Notaries						

none						
Auditors						
2017	**37**					
Bailiffs						
2017	**25**					
Trust and company service providers						
2014	**2**		**2**	**14 122**		
2015	**2**		**2**	**2 290**		
2016	**1**		**1**	**2 672**		
Total	**5**		**5**	**19 084**		

Impact of supervisory actions on compliance

The Czech National Bank (CNB)

469. There is a positive impact of the CNB supervisory actions on compliance, mainly in stimulating the FIs to correct the identified breaches. The CNB accentuates the importance of remedial actions, and pays attention to the subsequent regular monitoring, which contributes to the improvement of AML/CFT compliance culture.

470. The interviews with the private sector revealed a common understanding that in general the AML/CFT breaches would not lead to any significant pecuniary sanctions, provided that the obliged entity would demonstrate its willingness to remediate the shortcomings in a timely fashion. This, in itself, it is a positive outcome. The difficulty appears in relation to the CNB's capacity to actually discover possible AML/CFT compliance breaches for all FIs. Although the remedial measures (for breached that have been identified) have a positive impact, in the absence of dissuasive fines, sustainable and effective self-compliance efforts by the FIs are not ensured. Pecuniary sanctions are not playing their dissuasive and deterrent role and they are not applied in a proportionate manner.

471. Financial sectors with high number of obliged entities (e.g. insurance intermediaries, non-banking payment services providers or electronic money issuers, etc.) are subjects to a limited number of audits. For them, the supervisory actions have limited impact on compliance.

Financial Analytical Office (FAU)

472. Similarly to the CNB, there is a positive impact of the FAU supervisory actions on compliance. By conducting on-site inspections, the FAU determines whether the reporting entity fulfils the obligations given by the AML Act and, if it finds deficiencies, the FAU is applying correctional measures.

473. In general, the AML/CFT pecuniary sanctions imposed by the FAU do not play a deterrent role, as they are not regularly used, neither dissuasive.

474. The sanctions were not applied proportionally throughout the financial sector. For example, the evaluation team considers the fines applied to exchange offices more dissuasive (keeping the proportions) than those applied for other FIs. In 2016, fines in total amount of EUR 28.626 were applied by the FAU to 9 exchange offices (approximately EUR 3,180 per exchange office) and EUR 32,282 EUR in 2017 to 11 exchange offices (approximately EUR 2,934 EUR per exchange office) for

CDD and failure to ask information about the origin of the funds. This appears to the evaluators to be more dissuasive, taking into account the size of the business, in comparison to sanctions applied by FAU to other obliged entities, especially banks.

475. The comment related to the CNB's capacity to actually perform on-site visits and to draft recommendations in each and every case of AML/CFT compliance breaches applies to the FAU.

Supervisors of DNFBPs - Czech Bar Association, Chamber of Tax Advisers, Notarial Chamber, Bailiff Chamber, Chamber of Auditors

476. The supervision performed by the Czech Bar Association, Chamber of Tax Advisers, Notarial Chamber, Bailiff Chamber, and Chamber of Auditors in the sphere of AML/CFT is not at the stage where it can prove effect on AML/CFT compliance. This is complicated by the fact that often, the legal professions might play a certain role in integrating foreign assets into the Czech economy, as they are involved in the creation and/or administration of legal persons and legal arrangements. Auditors, accountants and tax advisors have close relations with their clients and are able to identify misuse of corporate vehicles. Nevertheless, the legal professions met on site demonstrated a limited knowledge on how corporate vehicles can be abused (IO4), which is reflected in the poor level of suspicious transactions reporting. The assessment team believes that more focused supervisory action is necessary to remedy the matter.

Other DNFBPs

477. With regards to other DNFBPs, little evidence was provided that supervisors, as far as they exist, have a positive effect on compliance with the AML/CFT obligations by the obliged entities.

Promoting a clear understanding of AML/CTF obligations and ML/TF risks

The Czech National Bank (CNB)

478. The CNB participated in several AML/CFT conferences and seminars (20 for 3 years) where senior inspectors provided trainings to the representatives of the private sector (mainly to AML/CFT Compliance Officers) on the new development of the AML/CFT framework. Apart from the regular meetings, ad hoc meeting with representatives of supervised institutions are arranged if necessary.

479. The CNB also operates a website[68] dedicated to AML/CFT matters, which provides i) basic information on AML/CFT requirements, ii) legislation, and iii) an updated review of recommendations for the financial institutions to avoid the most common shortcomings which have resulted from the on-site inspections.

480. CNB's supervisory experience and common findings are regularly discussed with the representatives of the SRB (e.g. Association of Czech Insurance Brokers, Association of Financial Intermediaries and Financial Advisors of the Czech Republic, Association of Currency Exchange Offices[69] etc.).

[68] http://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/20131010_opatreni_proti_legaliz_vynosu_trest_cin.html (available in Czech only).

[69] In June 2017 a meeting with the newly established association of currency exchange offices took place. Their representatives were informed about the most frequent supervisory findings from the AML/CFT area, as well as about the experience of inspectors supervising the proper fulfilment of these obligations.

481. As more extensively described under the IO4, the FIs confirmed that the CNB actions in promoting a clear understanding of the AML/CFT obligations are of added value.

Financial Analytical Office (FAU)

482. The FAU is active in the field of AML/CFT education, routinely organising training and providing opinions for the obligated entities and professional organisations (15 seminars for 3 years). Obliged entities may ask the FAU for written opinions, or use telephone consultation if need be. Selected views on the most frequently asked questions are published on the FAU's website and serve to raise awareness of the obligations under the AML/CFT Act and other relevant legislation.

483. The FAU issued several methodological guidelines providing interpretation of the AML/CFT Act, (*i.e.* identification of the beneficial owner, and CDD for the gambling operators; identification of clients without his/her physical presence; STR submission; preparation of internal rules etc.). The legal department of the FAU regularly updates these methodological guidelines.

484. The FAU promotes the approach that FIs and DNFBPs should not reject a risky client, as this would push him/her to move into the informal system. Through the risk-based approach, the reporting entities should take proportionate measures and, in case of doubt, consult with the FAU and/or submit an STR. Such approach creates the conditions for financial institutions and DNFBPs for accepting all clients disregarding the risks and vulnerabilities of usage of instruments of fictitious entrepreneurships and the vulnerability of integration of foreign criminal assets into the Czech economy.

Supervisors of DNFBPs - Czech Bar Association, Chamber of Tax Advisers, Notarial Chamber, Bailiff Chamber, Chamber of Auditors

485. The Chamber of Auditors of the Czech Republic organizes regular trainings for its members (auditors and audit companies) in order to provide up-to-date information on AML/CFT issues and to familiarize the auditors with the procedures described in the Internal Guidance on dealing with AML issues issued by the Chamber.

486. Training for lawyers and legal trainees was organised by the Czech Bar Association. The Czech Bar Association issued the AML/CFT Assessment Guide which is regularly updated.

Conclusions

487. The CNB has a robust FIs licensing mechanism, including a sound process to make sure that criminals are not owners or managers of financial institution. Some deficiencies have been identified in relation to the ability to recognize PEPs and associates of criminals in the authorisation process. The AML/CFT Chief Compliance Officers of credit institutions are not subject to any mandatory qualification requirements or “fit and proper” tests. For gambling business, the basic license is issued by the Ministry of Finance, which verifies the provided data using publicly available sources. The real estate agents, accountants, trust and company service providers, dealers in precious metals and stones and traders in items of cultural heritage or items of cultural value are not subject to licencing and hence, no measures are in place to prevent criminals and their associates from being professionally accredited or holding a significant or controlling interest, or a management function in these DNFBPs.

488. The FAU and the CNB have a good understanding of ML/FT risks in the Czech Republic. The two main supervisors demonstrated significant efforts in promoting the results of the risk

assessment amongst the entities under their remit. On a less positive side, both the FAU and the CNB have very limited human resources responsible for AML/CFT supervision which, in the opinion of the evaluation team, constitutes a limitation of the supervisory capacities and negatively impacts the effectiveness. The representatives of the professional Chambers demonstrated a satisfactory level of understanding of AML/CFT risks. The General Customs Directorate has a basic understanding of risks as it has only started performing supervisory function since 2017.

489. CNB`s Financial Market Supervision Department applies a comprehensive AML/CFT risk-based supervision system (RAS/RAS II) which is to a lesser extent implemented by the CNB Financial Market Supervision Department II . The model used by the FAU to determine the frequency and depth of on-site audits does not consider individual institution risk or risks assigned for groups of institutions within particular sectors. The criteria used by professional Chambers for inspections planning do not contain specific ML/FT components. General Customs Directorate does not apply any specific AML/CFT risk based tools.

490. Pecuniary sanctions applied by the FAU and the CNB are not playing their dissuasive and deterrent role and they are not applied in a proportionate manner. The on-site interviews revealed that AML/CFT breaches in general would not lead to any significant pecuniary sanctions, provided that the obliged entity would demonstrate its willingness to remediate the shortcomings in a timely fashion. Although the remedial measures have a positive impact, in the absence of dissuasive fines, sustainable and effective self-compliance efforts by the FIs are not ensured. Supervision by Professional Chambers is not at the stage where it can prove an impact on AML/CFT compliance by legal professions.

491. The FAU and CNB continuously perform significant efforts in promoting a clear understanding of AML/CTF obligations and ML/TF risks.

492. **Czech Republic has achieved a moderate level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

- The Public Register in the Czech Republic, include several Registers including the Commercial Register (CR), the Register of Associations, the Register of Foundations, the Register of Associations of Unit Owners and the Register of Benevolent Associations. Evaluators note that in the Czech Republic it is fairly easy to establish certain types of companies or to buy ready-made companies for a low price.

- Every public register can be accessed directly and free of charge through the internet and, upon request, the public authorities can require non-public information (such as copies of the documents) which is provided in a timely fashion.

- LEA and Prosecution consider the CR a good tool, significantly improved since 2017, and they routinely use this source in the course of a criminal investigation. However, it was acknowledged that the quality and accuracy of information may vary despite the constant improvement in the system. In case inaccuracies are detected, the Registry Court is petitioned and administrative, rather low level sanctions are applied. Under specific circumstances, both legal and natural persons may face criminal charges for providing grossly misrepresented or false statements in the documents submitted to the Public Register.

- Trust and BO Registers have been recently introduced but are still not fully populated with the respective data and information.

- Misuse of trusts is considered as bearing a moderate risk in the NRA. However, the number of trusts formed has begun to increase in recent years.

- Turning to potential abuse of legal entities for ML/FT purposes, the evaluators are not convinced that relevant competent authorities have fully assessed the vulnerabilities of all legal persons that can be created in the country. There have been cases of successful abuse of legal entities for the purposes of money laundering, including through use of shell companies.

Recommended Actions

- The authorities should carry out a comprehensive analysis of risks associated with all types of legal entities. The analysis should, *inter alia*, take into account the typology of using "straw men" to incorporate and execute financial transactions through corporate vehicles.

- Measures should be in place to enable the registrars of basic and beneficial ownership information to be able to verify whether information provided to them is adequate, accurate and current; this framework should be actively implemented by the registrars.

- Training programmes for LEA, supervisors and the reporting entities targeting the nature and operations of legal arrangements should be held with the aim to enhance their capacities to better comply with the AML/CFT obligations.

- Sanction applied to the entities which fail to supply adequate, accurate and up to date basic and beneficial ownership information, or fail to supply information in a timely manner, should be more dissuasive.

- Training programmes and specific AML/CFT guidelines to the legal professions involved in the establishment and/or management of legal persons should be developed to enhance their awareness and understanding of the application their AML/CFT obligations and the sector specific risks.

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

493. As noted under paragraph 117 and Table 2, there are three types of legal persons that can be established according to the Czech private law - corporations, endowed institutions and institutes. Legal persons established under public law (for example state owned enterprises) and some foreign types of legal persons are also permitted to operate in the Czech Republic.

494. The process of establishment of business corporations is described in the web site of the Czech Trade Agency[70]. Information on other types of legal persons is provided on-line[71]:

495. The evaluators noted that in the Czech Republic it is fairly easy to establish certain types of companies or to buy ready-made companies for a very low price. The assessment team has not been provided with statistics on number of legal persons with foreign ownership.

496. All legal persons must be registered in a public register. The company name, corporate structure, legal form and status, the address of the registered office, basic regulating powers, a list of directors and financial statements of legal persons are mandatorily recorded. The Public Register of Legal and Natural Persons includes the Register of Associations, the Register of Foundations, the Register of Associations of Unit Owners, the Commercial Register, the Register of Publicly Beneficial Associations and the Register of Trusts. The Register of Trusts is partly public, is accessible from the Ministry of Justice web site, and provides data on trustee(s), settlor(s), beneficiary (ies) and protector(s). The information registered in the BO Register will be accessible only to qualified users, such as law enforcement authorities or the tax administration. The registration process started on 1 January 2018 and it was not completed at the time of the on-site visit.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

497. The authorities' understanding of potential misuse of legal entities and legal arrangements for ML/FT purposes derives from the NRA process (to which they contributed) and the NRA report (which draws the integrated conclusions from all parties involved). The NRA reviews the risks associated with several types of legal entities (e.g., NPO, offshore structures, complex structures of companies), and provides some typologies of abuse of the entities. Limited liability companies are considered to be the most vulnerable types of legal persons due to their share in the total number of the entities, and the portion in the corporate portfolio of banks.

498. The NRA analyses the use of shell companies and off-shore companies mostly in relation to tax evasion and public procurement crime, but does not place much emphasis on "straw men" involved in the establishment of a significant number of companies.

499. At the same time, the NRA does not review vulnerabilities of different ownership structure of legal persons, and does not consider risk associated with foreign entities, which are administered in the Czech Republic and have bank accounts in the country.

[70] http://www.businessinfo.cz/cs/clanky/zapis-do-obchodniho-rejstriku-ppbi-24147.html#!&chapter=1
[71] https://seznam.gov.cz/obcan/zivotni-situace/obcan-a-stat/obcanske-aktivity/zalozeni-spolku.html.

500. Separate sections of the NRA are devoted to the ML/FT abuse of NPOs. Specific nature of NPOs is described, together with vulnerability and suspicion indicators. The analysis appears to be adequate but lacks typologies.

501. Complex legal structures such as trusts, together with the difficulties encountered in ascertaining the ultimate beneficial owners of trusts are analysed in the NRA. Misuse of trusts are considered as bearing a moderate risk in the NRA, although in practice they increased in number over years and no supervisory actions have been taken. However, the number of trusts formed has begun to increase in recent years.

Table 19: Number of registered trusts in CzR

Trusts	In 2012	In 2013	In 2014	In 2015	In 2016	30. 6. 2017
Total	0	0	49	155	310	406

502. While approximately half of the STRs submitted to FAU concern legal persons, the extent of abuse of legal persons in relation to prevailing types of crime is not quantified, and LEAs did not provide statistics on the value of confiscated company shares, therefore the magnitude of the problem has not been assessed. Representatives of the Prosecutors, FAU and CNB appreciate the efforts made to improve transparency of companies, trusts and beneficial ownership. LEAs demonstrated general knowledge of the ML/FT threats, vulnerabilities and consequences with regards to legal persons.

Mitigating measures to prevent the misuse of legal persons and arrangements

503. The misuse of legal persons and legal arrangements can be substantially prevented if information on the legal owner, the beneficial owner and the nature of business activity were available to the competent authorities. Therefore, the competent authorities made steps to improve transparency of legal persons and arrangements, and strengthen supervision thereof. Introduction of the Register of Beneficial Owners, the Register of Trust and the Register of Bank Accounts are the most noteworthy achievements, appreciated by the investigating authorities.

504. The Public Register is managed by the Register Court and all types of legal persons established under the private Law are obliged to list themselves. The law enforcement authorities interviewed on-site maintained that the quality and accuracy of the registry data have improved significantly since 2010. The mandatory information for registering the company include the name, corporate structure, legal form and status, the address of the registered office, basic regulating powers and a list of directors. The companies are responsible to notify the court about the changes in the management or ownership structure. All public registers can be accessed directly and free of charge through the internet and, upon request, the public authorities can require non-pubic information (such as copies of the documents). These documents, upon request by the authorities, are provided in a timely fashion.

505. Financial institutions and DNFBPs are satisfied with the content of the Public Register, its user-friendly interface and search tools, but some of them expressed concerns about the accuracy of the data. Financial institutions and DNFBPs do not seem to notify the court when discrepancies are identified in the database. LEAs and the Register Court estimate inaccuracy of data in the register to be between 10%-20%, while most of the financial institutions and DNFBPs believe that the data is rather reliable. The Register Court receives feedback about the data in the Public Register mostly from the tax authority and the Office of Prosecutors. The Court checks if the provided information corresponds with the filled documentation and with the identity of natural persons which are registered. The Court does not have an authority or obligation to verify the correctness of the information provided.

506. The assessment team positively notes that in 2015, based on information pertaining to potential ML/FT risks received from state authorities, the City Court of Prague (by far the biggest Registrar Court in the Czech Republic) appointed three judges to de-register inactive companies. As a result 6,000-7,000 entities are de-registered annually, which significantly contributes to an increased accuracy and reliability of the database.

507. According to the Czech law, a company may issue bearer shares only as book-entry securities or immobilised securities. Bearer shares that have not been immobilised or converted to book-entered bearer shares before 2014 have been converted automatically into registered shares.

508. Although the Czech law does not provide for the concept of nominees, the legislation does not prohibit a person from acting as a nominee director or shareholder. During the on-site interviews, the evaluation team did not identify any elements leading to the conclusion that the concept of "nominee" is used in practice. In the absence of legal provisions regulating officially the "nominees" they can be intertwined with the concept of "straw men"[72]. As captured and analysed in IO5 and IO1 above, typologies including "straw men" were developed by FAU but this vulnerability was not enough explored in the NRA.

509. The Register of Beneficial Owners was created as of 01.01.2018, and at the time of the on-site visit the Register was not yet operational (according to the authorities approximately 300 inputs have been recorded by March 2018). The deadline for the existing business corporations to register their beneficial owners is within one year from the date of entering into force of the Public Registers Act, i.e. until 1 January 2019. Other legal persons registered in the Public Register (i.e. associations) are obliged to register an ultimate beneficial owner within 3 years from the date of effect of the Public Registers Act, i.e. until 1 January 2021. The newly incorporated legal entities (after 01.01.2018) have to register without undue delay their BO.

510. Legal professions are involved in the creation and/or administration of legal persons and legal arrangements. Auditors, accountants and tax advisors have close relations with their clients and are able to identify misuse of corporate vehicles. Nevertheless, the legal professions met on site demonstrated limited knowledge on how corporate vehicles can be abused (IO4), which is reflected in poor level of ST reporting. The assessment team believes that more focused supervisory action is necessary to remedy the matter. TCSPs have a marginal role in the formation and administration of legal persons in the Czech Republic. Trusts are used in practice for the management of large family assets and their intergenerational transition, and to achieve a specific business plan of several entities, instead of an association of entrepreneurs in a business consortium, to support a sports club or for similar purposes.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

511. All existing public registers can be accessed directly and free of charge through the internet and, upon request, the public authorities can require non-pubic information (such as copies of the documents) which is provided in a timely fashion.

512. The authorities primarily rely on banks to obtain the beneficial ownership information when a BO is not the same as the registered legal owner. The domestically-incorporated legal entities do have bank accounts with Czech banks as this is needed for tax purposes. The prosecutors met onsite

[72] See FATF EGMONT GROUP report "Concealment of beneficial Ownership" report page 6. http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Egmont-Concealment-beneficial-ownership.pdf

stated that they had direct access to the Registry of Bank Accounts and expressed satisfaction with the improved quality of beneficial ownership information held by banks. Certainly, the limitations related to the reliability of BO information described in IO4 apply, but the authorities did not point any problems encountered in retrieving the necessary data. Depending on the situation, the request can be made directly to the bank or through the FAU (i.e. if the case was initiated based on a FAU disclosure). The prosecutors also informed the assessment team that they already tested the under-construction BO Registrar and that the results were obtained in 15 minutes..

513. Police use the same mechanisms to obtain BO information and did not report problems in retrieving the necessary data on beneficial ownership from banks, which was described as a regular practice. However, they also advised that in case of investigation of more complex schemes involving movements of funds between multiple domestic and foreign companies, identifying beneficial owners of the latter (those which do not hold bank accounts in the Czech Republic) gets more complicated and often requires international cooperation. However, another avenue for the competent authorities to obtain basic and BO information are the legal professions involved in the incorporation of legal persons (such as notaries and lawyers). They are also REs under the AML/CFT Law and subject to the same CDD and record keeping requirements as the banks. LEAs make less use of these, as access through the banks is simpler.

514. The quality of data mostly depends on the diligence of the registered entity and changes are only based on notifications by the entity. Therefore, there is a serious concern that the Register of Beneficial Owners may fail to provide accurate and up to date information. No fines are provided for a false declaration or failure to declare, hence, there are no significant safeguards against false declarations of BO in the registrar.

515. In addition to the Registrar, competent authorities can obtain information on legal persons and beneficial ownership from the reporting entities performing CDD. All legal persons and legal arrangements are required to establish a relationship with a bank for tax and other purposes. Until recently, this process was rather slow, as at an initial stage, LEAs did not know which financial institution or DNFBP held data about the specific corporate vehicle. With the introduction of the Registry of Bank Accounts, the process is significantly speeded-up made by the easiness in identifying the respective bank. As discussed in IO4, CDD and beneficial ownership data maintained by banks is generally accurate and reliable. When ownership structure is more complex, and involves foreign legal or natural persons, foreign counterparts can be applied to identify the beneficial owner.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

516. At the time of the on-site visit, there are 406 trusts incorporated in the Czech Republic. Similarly to the BO Registrar, the Register of Trust was created beginning of 2018. New trusts are required to register while for the existing ones the process of data-input was on the way. The process is to be finalised in 2018. The Register Court administers the Register of Trusts similar to the Public Register. Information on the trustee, settlor (founder), beneficiary and protector has to be recorded in the Register of Trusts. Once operational, the Registry will be accessible to qualified users (law enforcement, supervisors…).

517. Legal arrangements have to register BOs in the Register of Beneficial Owners.

518. Until the Register of Trusts will be operational, information can be obtained only from the reporting entities. Reporting entities met on site considered trusts as risky clients due to the nature

their activities and demonstrated high due diligence in identifying the parties concerned and the purpose of the establishment of the Trust. As anecdotal evidence, one of the interviewed banks was able to quote on the spot the actual number of Trust clients they had, as well as and their profile (family assets management). LEAs mentioned challenges in the identification of beneficial owners of trusts, although not many cases have been reported. It appeared that the challenges were more due to the novelty of the concept and lack of practice in the area than due to actually lack of basic and BO information.

519. To support financial institutions and DNFBPs in identifying beneficial owners of trusts, FAU published Methodological Instruction 3 "Determining the beneficial owner by obliged entities", which has a chapter on trusts. The FAU supervises the Trusts for AML/CFT compliance and in the course of the supervisory activity fines have been applied for the breaches identified (see Table 18). Nevertheless, the reporting entities do not seem to have an overall picture on the nature and operations of trusts. Therefore, adequate, accurate and up-to-date ownership information may not be quickly available to the relevant interested parties.

Effectiveness, proportionality and dissuasiveness of sanctions

520. The Register Court does not conduct regular checks of the records in the Public Registry. Discrepancies in records are advised to the Register Court when identified by the Prosecutor's Office, the Tax Authority and/or private sector entities. In such cases, the court sends a written warning to the entity, urging it to correct/update the records and if the entity fails to do so, the court may impose a fine or, when relevant, launch the process of its dissolution.

521. No statistics on the imposed sanctions have been provided by the Registry Court (which includes the Trust Register) to the assessors, but the interviews demonstrated that pecuniary sanctions are rarely imposed, usually in case of repeated breaches. The pecuniary sanctions may amount to a maximum of 100,000 CZK (approximately EUR 4,000) which appears not to be effective and dissuasive. According to the Registry Court, the most serious sanction for legal companies for breaching the registration requirements is dissolution. However, seeing that in most of the cases the companies do not have any activity, this is hardly a dissuasive sanction. The authorities have not provided a case of dissolution of a company that was operational.

522. According to Section 9 Subsection 2 Letter a) of the Act No. 251/2016, on some Administrative Offences, a legal person or a self-employed natural person commits an administrative offence by not fulfilling the obligation to "submit an application for registration, change, or deletion of a record in the Commercial Register or another public register". The provision implies an administrative fine of up to 100,000 CZK (approximately EUR 4,000) for the above mentioned breaches which for a natural person can be considered as dissuasive. Statistics on the volume and number of the respective administrative sanctions were not available.

523. Under specific circumstances, based on Section 254 Subsection 2 of the CC, both legal and natural persons may face criminal charges for providing grossly misrepresented or false statements in the documents submitted to the Public Register. The charges can vary from dissolution of the entity, to imprisonment and/or financial penalties. In 2016, a total of 193 natural and 8 legal persons were charged for committing crimes which fall under the Section 254. However, the above statistics include breaches which do not concern the Public Register, hence they are not accurately illustrating the number of criminal charges brought in respect of false statements in the process of incorporation of a company.

524. The Registry of Beneficial Owners is also administered by the Registry Court, but no supervision or sanctions are applied to corporate vehicles for submitting inaccurate data upon registration, or for failure to update the BO in the Register of Beneficial Owners.

525. The total value of sanctions applied by FAU and CNB for AML/CFT breaches ranges between 100,000 CZK and 1,000,000 CZK (approximately EUR 4,000 – EUR 40,000). Whilst these sanctions may be applied repeatedly, most of them were imposed for failure to apply full CDD measure and perform BO identification. As discussed under IO3, the number and the volume of the pecuniary sanctions imposed so far are not dissuasive enough. No sanctions have been imposed to the DNFBPs for AML/CFT breaches.

526. As described under Recommendation 24, the reporting entities have the obligation to provide the FAU with basic and BO information and failure to do so is subject to sanctioning. No such cases have been reported by the authorities. Based on a Court order, FIs and DNFBPs are obliged to provide law enforcement with beneficial ownership information but no evidence on the timelines was provided to the evaluation team.

Conclusions

527. The existing Public Registrar and the under-construction Registrars of BOs and Trusts constitute a positive move towards a transparent and open culture in respect of legal persons and arrangements. Whilst information on legal persons is publicly available and can be obtained from the Public Registrar, information on BO and trusts can be obtained from the reporting entities.

528. The NRA reviews the risks associated with a few types of legal entities, and provides some typologies of abuse of the entities. However, the vulnerabilities related to different ownership structure of legal persons are not comprehensively reviewed, and the risk associated with foreign entities is not considered.

529. All types of legal persons established under private law are obliged to register in the Public Register in the CR. The law enforcement authorities maintained that the quality and accuracy of the registry data have improved significantly in the last years. The Court does not have an authority or obligation to verify the correctness of the information provided, but the assessment team positively notes that the City of Prague Registry Court appointed three judges to dissolve inactive companies. This measure is expected to significantly contribute to an increased accuracy and reliability of the database.

530. All existing public registers can be accessed directly and free of charge through the internet and, upon request, the public authorities can require non-pubic information (such as copies of the documents) which is provided in a timely fashion. Effective, proportionate and dissuasive sanctions were not imposed to the legal persons and legal arrangements for providing inaccurate data or for not failure to notify about relevant changes to the Registry Court. **The Czech Republic has achieved a moderate level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

- The Czech Republic (CzR) authorities have been active in relation to foreign requests, including those related to seizing and freezing assets. The issue of timelines for MLA is difficult to assess based solely on statistical information, which is incomplete. However, the feedback received from other jurisdictions was largely positive in terms of quality of MLA and did not highlight the timeliness as an issue of concern.

- The authorities have also demonstrated significant activity with respect to the outgoing MLA requests across all predicate offences. The number of outgoing requests regarding ML offence also demonstrates that the authorities are proactive in seeking assistance from abroad. Nonetheless, since the underlying offence is not identified for the majority of requests sent, it cannot be concluded with certainty that the ML requests sent abroad are entirely in line with those found to represent the greatest risk for ML in the CzR.

- The FAU proactively and constructively cooperates with its foreign counterparts by exchanging information on ML, associated predicate offences and FT, both spontaneously and upon request. Police and intelligence agencies are engaged in continual cooperation with their foreign counterparts. This includes cooperative information sharing via different multi-agency platforms as well as cooperation at the operational level (e.g. actively taking part in joint investigative teams).

- Whilst the assessors have not noted any impediments in providing assistance related to BO information, the quality and accuracy of available information in this area may limit the scope of effective international cooperation.

Recommended Actions:

- Authorities responsible for MLA and Extradition should establish more complete systems for tracking the number and nature and delay in relation to their cases, particularly in respect of ML matters and their predicates;

- Whenever assistance on outgoing requests to certain jurisdictions is found as problematic, relevant CzR authorities should engage in more frequent consultations with foreign authorities in order to seek solutions to these problems;

- Based on their knowledge of the legal requirements of various jurisdictions that they have dealt with, CzR authorities should put in place training lectures for the appropriate Czech stakeholders, including police, prosecutors and judges as the case may be.

Immediate Outcome 2 (International Cooperation)

Providing constructive and timely MLA and extradition

531. The CPC and the Act on Judicial Cooperation in Criminal Matters (IJCCM) create a comprehensive legal framework for the MLA and extradition, which enables the authorities to

provide the widest possible range of assistance in relation to investigations, prosecutions and related proceedings concerning ML, associated predicate offences and FT.

532. The Czech Republic has in place 44 bilateral treaties for MLA and extradition covering not only European neighbours, but also countries around the world. A number of multilateral instruments are in force, facilitating international cooperation. In the absence of a treaty, extensive MLA may be provided on the basis of reciprocity. Different examples of such reciprocity-based co-operation were presented to the assessment team. These included cases where cooperation was sought by Iran, Singapore Philippines, Brazil, Jordan and SAE, some of them involving the application of freezing measures which were executed. As for treaty based cooperation with non-EU states, the authorities underlined that the most frequent cooperation based on bilateral treaties is the one with the United States. Cooperation with European states that are not members of the EU is executed mostly through the relevant Council of Europe conventions. The various treaties signed by the CzR and the country's ability to respond to requests across a broad range based on reciprocity, even in the absence of an applicable treaty have a direct and positive impact on effectiveness by increasing the CzR ability to respond to incoming requests. Examples of successfully executed requests based on reciprocity were provided to the assessors.

533. Importantly, the Czech Republic has, since the last evaluation, ratified and implemented to a great extent, the United Nations Convention against Transnational Crime ("Palermo Convention") and the United Nations Convention against Corruption ("Mérida Convention"). While there remain minor issues with complete criminalisation of ML and FT which might have a negative impact on the ability to provide assistance where dual criminality is required, in terms of effectiveness, in the assessment team's view these would impact very few cases.

534. Over the last few years Czech authorities have maintained a high level of activity in relation to incoming requests for MLA based on all offences that have been received in increasing numbers[73]:

2014 – 2851 MLA requests received

2015 – 2817 MLA requests received

2016 – 3369 MLA requests received

2017 (partial statistics) – 1828 MLA requests received

535. Czech authorities maintain that the great majority of MLA requests received have been executed and most within 1-2 months, and extradition requests on average within some 13 months, unless another specific timeframe was indicated by the requesting party. Although this general statement does not appear to be based on a careful case-by-case review (as the Czech Republic does not yet have in place an integrated nation-wide case management system), the feedback received from other jurisdictions about the promptness and general quality of the assistance provided by Czech authorities is quite positive in general. In addition, the International Department of Supreme Public Prosecutor´s Office, as the Central Authority dealing with all (non EU) MLA cases is in a position to have an overview of such cases. This same Department executed a partial review of the delays regarding incoming MLA requests received from EU partners where these were executed by subordinate Regional Offices. The overview and the partial review add support to the estimate for execution times, which are in an acceptable range.

536. The Czech Republic not only has the legal means to maintain confidentiality, but its authorities are under a positive legal obligation to do so, which goes beyond the requirements of Rec. 37.5.

[73] These figures concern the overall number of requests for all crimes.

Operationally, the relevant authorities have all been made aware of this duty and take the matter seriously when handling MLA requests and any responses thereto.

537. A description of requirements to be met by the requesting state so that the Czech Republic can execute the MLA or extradition requests is available on the website of the EJN (for EU Member States) or the PC-OC (for Council of Europe members). Prosecutors and judges may cooperate directly with their peers from other EU countries, whilst in the case of other jurisdictions the communication is done through the central authorities. These measures increase effectiveness.

538. Dual criminality is required only if the MLA request involves coercive actions. All MLA requests are executed under the same conditions as are applied in the domestic criminal proceedings. There are no provisions which would impede or hinder international cooperation. The execution of a MLA requests is refused, infrequently, for example, where a requesting country does not provide sufficient grounds for the execution and fails to provide supplemental information; where it is impossible to locate the person to be interviewed; where the request concerns an action requiring dual criminality which is not established in the given circumstances; or where it does not meet the criteria for authorisation of the action under the CPC. These grounds of refusal do not negatively impact effectiveness.

539. The following table shows partial statistics on the number and nature of some of the requests received, focusing, for MLA, on ML and particularly relevant predicates but without detailed information on the nature of extradition requests in recent years. The extradition requests in this table include only those sent/received to/from non-EU member states.

Table 20: MLA and extradition requests received (2012 – July 2017)

	Received		**Pending**		**Refused**		**Executed**		**Average time of execution(days)**	
	MLA	**Extradition**	**MLA**	**Extradition**	**MLA**	**Extradition**	**MLA**	**Extradition**	**MLA**	**Extradition**
2012		13	Not available (N/A)	32	N/A	6	(N/A)	8	N/A	13,5
2013	56	12	N/A	32	N/A	8	N/A	5	1-2 months	16,5
2014	119	23	N/A	46	N/A	13	N/A	5	1-2 months	17,5
2015	142	22	N/A	N/A	N/A	12	N/A	5	1-2 months	13,5
2016	157	16	N/A	38	N/A	10	N/A	11	1-2 months	19
30.6. 2017	94	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1-2 months	N/A

540. With respect to requests relating to the freezing, seizure and confiscation and sharing of assets in response to MLA, little statistical data is available, although some examples of such successful cooperation were provided (please also see the cases included below in the section on FIU-to-FIU cooperation):

Request from France

In 2013, based on the COE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), France requested confiscation of funds (up to 1 million CZK/EUR 38,780) on a specific bank account in the Czech Republic in execution of a criminal judgment issued in France as a sanction for conviction of solicitation- related money laundering. The French Court order was recognized and confiscation of approximately 370,000 CZK (EUR 14,348) executed in the course of 2014 with subsequent sharing in 2015, under s. 135 IJCCM. Half of the money went to France, the remainder kept by the Czech Republic in order to cover costs of proceedings.

Request from Switzerland

In 2012 Switzerland sought confiscation of money on Czech bank accounts which had been previously seized based a Swiss MLA request. Based on the European Convention on Mutual Assistance in Criminal Matters of 1959 and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime from 1990, the Swiss criminal confiscation order (for 27,000 CZK and EUR 3,500) was enforced and the funds confiscated. The crime included the offences of economic espionage, ML, breach of bank and trade secrecy.

541. Czech authorities also provided information about outstanding requests from several different countries, including one where a non-conviction based order is sought to be executed under s. 101 of the Czech CC, but since these matters were in progress at the time of the on-site, details could not be provided.

542. Data provided by the Czech authorities show that incoming requests for extradition are dealt with swiftly when they are made by members of the EU since the principles of the European Arrest Warrant have been incorporated into Czech law. For non-EU countries the process is slower but still within an adequate range. Virtually no negative comments were received in relation to the performance of Czech authorities in this regard. In addition, the authorities presented several cases where the Czech Republic acted had received (non EU) requests for extradition.. Most of these extradition requests were based on the Council of Europe Convention on Extradition (1957). One case with US, which was carried out based on the bilateral treaty signed with the Czechoslovak Republic, was based on several charges, including conspiracy to commit ML. This extradition request was executed in 8 months, which is not considered excessive given the complexity of the matter.

Seeking timely legal assistance to pursue domestic ML, associated predicate and TF cases with transnational elements

543. Partial statistics were provided in relation to outgoing MLA requests related to ML and certain predicates. However, since the requests on ML did not include reference to the underlying offences, it is difficult to conclude that these requests properly respond to the need to seek assistance in accordance with the Czech Republic's risk profile in terms of the nature of outgoing requests. It is noted that, while Czech authorities (investigators, prosecutors) made reference to unsuccessful attempts to obtain MLA from abroad, the table below shows no information on the number or basis in relation to refusals of Czech MLA requests. The authorities provided a small number of examples of refusals indicating that some countries did not execute their requests given the small amounts involved (e.g. EUR 4,000.00) or that the requested country would not accept a Czech request written in English, which was not that country's official language. Still there is an adequate number of requests pertaining to ML. Regarding extradition there is no information on the offence related to the outgoing requests, except for a few examples that did not concern ML, but did touch upon drugs and embezzlement, which are high-risk offences for the Czech Republic.

Table 21 MLA and extradition requests sent (2012 – July 2017)

	Sent		Pending		Refused		Executed		Average time of execution(days)	
	MLA	Extradition	MLA	Extradition	MLA	Extradition	MLA	Extradition	MLA	Extradition
2012		23		39		6		5		11,5
2013	86	12		40		6		5		20
2014	136	15		43		1		16		9
2015	177	11		N/A		3		12		17
2016	253	14		46		2		5		8,5
30.6.2017	209	N/A		N/A		N/A		N/A		N/A

544. For outgoing requests seeking freezing or confiscation of assets, Czech authorities did provide some statistical information which shows that in period 2013 – 2017 the incoming requests amounting up to 4.370.000,00€ were executed by the Czech authorities with regard to foreign ML cases. No details whether these were seized or confiscated funds were provided.

Seeking and providing other forms international cooperation for AML/CFT purposes

LEAs cooperation:

545. Supreme Public Prosecutors Office appointed (in 2016) the National Correspondent for combating terrorism, extremism and hate crimes and the National Correspondent for combating financial crime and money laundering, search and draining of proceeds from crime and for protection of financial interests of the EU. National Correspondent, or his expert team, not only form a point of cooperation for the National Member in Eurojust in the given area, but also serve as a guarantor of interdepartmental cooperation and cooperation with foreign countries. Currently there are a total of ten National Correspondents, appointed also for other areas.

546. The Czech Republic has 31 bilateral agreements on cooperation via the Ministry of the Interior with the foreign following jurisdictions. The general rules on processing information such as personal data are found ss. 79 – 88 of the Act on the Police. For incoming requests for police international cooperation, requests are made via different secured channels (SIENA, I24/7) or, in decreasing numbers, by regular emails or registered mail. Upon delivery each request is registered into ETR (the sole police case management system) and assigned a unique case file number. Confidentiality is maintained throughout the processing of such requests. Obtaining financial information from banks and other financial institution has been a time consuming and administratively demanding process, but since January 1, 2018 the new Bank Accounts register promises to greatly accelerate matters. Notwithstanding this fact, the access to this database is still subject to the prosecutor's approval. As already discussed under IO.8 the police have experienced no problem to swiftly obtain such approval and thus have not experienced any delays in obtaining bank account details. The limits of police cooperation set forth in s. 89 - 94 of the Police Act appear to be fully exploited in practice.

547. Czech authorities advise that joint investigation teams (JITs) are often used as a tool of international judicial cooperation and that 45 JITs agreements have been concluded since 2009 dealing with a variety of crimes.

548. The assessment team was provided with information concerning actual examples of police-to-police international cooperation, including details of a fruitful JIT involving Czech and UK police in relation to an insurance fraud and ML.

Case example - JIT between the Czech Republic and the UK

In 2013, based on the criminal complaint of one of the insurance companies, the Czech Police initiated an investigation which concerned the insurance and credit frauds. The suspects, with the intention of unlawfully obtaining financial means, created a chain of business relations within which they pretended to conduct real business activities. In this process they used valid insurance contracts which were covering the risks of outstanding debts arising from the financing of debts and liabilities. The insurance also applied to claims from bills of exchange (promissory notes) and to bills of exchange which the insured purchased before the date of their maturity. The suspects represented companies which were registered in the Czech Republic and the UK.

Between 2008 and 2012, on at least twenty-one occasions, the suspects made a claim for compensation and caused damages to banks in amount of CZK 1,139.949.994 (EUR 44,207,484).

The *modus operandi* was usually the same and only the credit insurance companies and banks were different.

Since some of the suspected companies and their representatives were located in the UK, the Czech prosecutor sent a MLA request to the UK. Meanwhile, in the UK, the Serious Fraud Office commenced an investigation for the suspicion of committing crimes of fraud by misrepresentation, fraudulent trading, false accounting, forgery, insurance fraud, and money laundering. The investigation was initiated following the referrals from two financial institutions, making allegations of fraud related to three companies registered in UK and the trade finance facilities they obtained for the purchase of steel and other commodities.

After receiving the request, the British authorities contacted the national representation at Eurojust and asked for a coordination meeting with the Czech authorities. The meeting took place in June 2015 and it concluded that there was a significant overlap between the two investigations, and that each party had relevant information. Both sides agreed to set up a JIT – this decision was enforced in August 2015.

The cooperation enabled exchange of crucial evidence and resulted in charges against four persons in the Czech Republic and six in the UK. Two main perpetrators in the UK have been charged for ML.

549. Police statistics related to the traffic between Czech police and their counterparts internationally via the ARO, CARIN and AMON networks were provided as follows:

International co-operation	**2012**	**2013**	**2014**	**2015**	**2016**		**30.6.2017**	
INCOMING REQUESTS	**total**	**total**	**total**	**Total**	**total**	**ML**	**total**	**ML**
Foreign requests received by LEAs	23	32	55	40	46	8	39	7

related to ML/FT[74]								
Average time of execution (days)	Urgent in 8h, other intelligence within 1 week, other information in 14 days	Urgent within 8h, other intelligence in 1 week, other information in 14 days	Urgent within 8h, other intelligence in 1 week, other information in 14 days	Urgent within 8h, other intelligence in 1 week, other information in 14 days	Urgent in 8h, other intelligence within 1 week, other information in 14 days	Urgent within 8h, other intelligence within 1 week, other information in 14 days	Urgent within 8h, other intelligence within 1 week, other information in 14 days	Urgent within 8h, other intelligence within 1 week, other information in 14 days
OUTGOING REQUESTS	**total**	**total**	**total**	**Total**	**total**	**ML**	**total**	**ML**
Number of requests sent abroad by LEAs related to ML/FT	95	87	93	92	111	11	95	31[75]

FIU to FIU cooperation

550. The FAU plays an important role in international cooperation in the CzR. The FAU proactively and constructively cooperates with its foreign counterparts by exchanging information on ML, associated predicate offences and FT. This is evidenced by the positive feedback received from foreign counterparts, as well as the growing number of spontaneous disseminations sent abroad by the FAU (see Table 22 below). Exchange of information is carried out both on the basis of a MOU[76] and based on the principle of reciprocity. The information provided by the FAU to the foreign counterparts may be used as evidence or intelligence, in other words the FAU, in general, does not condition the manner in which foreign counterparts may use the information provided. There seem to be no undue limitations either under legislation or in practice, which would hinder the provision of international cooperation.

[74] Procedure of the exchange information between AROs is stipulated in „Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union" (Swedish Framework Decision). According to section 2 (d) information and/or intelligence' is:
I) any type of information or data which is held by law enforcement authorities and
II) any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures, in accordance with Article 1(5).

[75] The increase of the number is caused by more cases of frauds on internet related to the ML. The increase is also influenced by slightly different approach to filling in the statistics when the officers were not used to include ML offence in many economic crimes and in 2017 this habit was developer. The statistic is also quite new and the system is being developed.

[76] The FAU has signed MOUs with Albania, Australia, Belgium, Bulgaria, Canada, China, Croatia, Cyprus, Estonia, France, Georgia, Ireland, Israel, Italy, Japan, South Africa, Kosovo, Lithuania, Latvia, Macedonia, Panama, Paraguay, Poland, Romania, Russia, San Marino, Slovenia, Slovakia, Serbia and Ukraine.

Table 22. Statistics regarding international cooperation of the FAU

	2014	2015	2016	June 2017
Requests of information sent by the FAU	260	254	297	131
Spontaneous disseminations sent by the FAU	154	328	469	323
Requests of information received by the FAU	200	164	275	168

551. During the period under review, the FAU received a large number of foreign requests, a significant portion of which were from neighbouring countries. Responses were provided to all of these requests. In the course of responding to foreign requests, and in accordance with the internal procedures, the FAU not only uses information directly accessible to it, but also seeks additional information from national authorities and obliged entities. Authorities indicated that requests are responded to within 20 days, whereas the time limit for urgent requests is 5 days. In exceptional cases the FAU may respond to the request immediately.

Case of FIU-FIU cooperation

In this case the aggrieved parties were from Belgium and France. Company B (limited partnership with unclear ownership structure, established in the United Kingdom) was originally a subject of Belgian FIU's request. This request was related to a bank account opened in a Czech bank in favour of which an attempt was made to fraudulently extract funds from the Belgian legal person. The company which tried to extract the funds opened 3 bank accounts in the CzR and the managing clerk of these accounts was a French citizen. After receiving additional information from the Belgian FIU, the FAU started the monitoring of these accounts. During the period when the accounts were monitored, the FAU received a STR regarding a payment in the total amount of EUR 462.922. The remitter was a large French company and the receiver was a French football club. The FAU then sent an urgent request to the Trackfin to verify this payment and perform checks on the subjects concerned. The FAU, Trackfin and Belgian FIU discussed the matter and continued to monitor the situation closely. The French company was soon contacted by the football club with a request to pay an invoice to their new bank account. This request was confirmed via e-mail which included an official letter from the football club and other relevant documents, all of which appeared to confirm the credibility of the sender. The French company, soon after ordering the payment in favour of the football club, received the information from the bank (and through the FAU and Trackfin), that the account to which the funds were transferred had been considered as suspicious and that the transaction was therefore blocked. Subsequently, it was confirmed that the football club had not changed its address, bank account or any other contact information. Then the management of the French company filed a criminal complaint with the French LEAs.

The FAU seized the total amount of EUR 463.038,- and filed also criminal complaint with Czech police based on the offence of legalization of proceeds of crime (Sections 216, 217 of the criminal Code) and fraud (Section 209 of the Criminal Code). The FAU also obtained and provided LEAs with information about the ID card used by the French citizen while opening accounts in the Czech Republic. This ID was reported as stolen in France. The IP address of the perpetrator was also detected and provided to police.

The investigation is underway, cooperation among Czech and French FIUs and LEAs is intensive and, at the time of the on-site, the setting up of JIT was in progress.

552. Whereas, the number of incoming requests has been fairly stable during the period reviewed, the number of outgoing spontaneous disseminations has been constantly growing, on the one hand due to the improvement of quality of the STRs received, and on the other - the FAU's policy in more actively engaging in cooperation with foreign counterparts.

International Cooperation – Cases when transactions were postponed

a) Postponement in the CzR

The FAU received a STR from obliged entity ensuring a payment service for company from country X. This obliged entity asked within the CDD procedure to submit the documents clarifying the origin of funds and the purpose of transactions. These documents were contradictory and the customer seemed nervous or even aggressive in the bank and asked for immediate transfer of funds as he ordered. The FAU detected in further analysis that in this case the transferred funds originated from tax crimes committed in country X. These findings were immediately shared with the country's X FIU and based on further communication it was detected that the country X already initiated criminal proceedings against two legal persons because of their business activity within an extensive international carrousel network with mineral oils. The purpose of this carrousel network was the VAT evasion. The country's X FIU asked the FAU to freeze the funds in Czech Republic which the FAU executed and froze the amount of CZK 51.000.000 (EUR 1,977,790).

b) Postponement abroad

In 2015 the FAU conducted analysis focused on the proceeds of crime from a corruption case. This analysis was initiated on the basis of the request submitted by the Czech Police. The FAU searched the proceeds of crime (estimated up to 1 mil. EUR) in the Czech Republic (bank accounts, immovable property, etc.) and abroad (requests to foreign FIUs) but failed to find any. The perpetrator was accused of corruption and the proceedings had already reached the hearing stage. The information about the proceedings was available from open sources. Based on the information from open sources the FIU of the country Y received a STR concerning the funds in the amount of approximately 250.000 EUR deposited in one of the banks in country Y. The perpetrator also intended to transfer these funds abroad. The FIU of country Y sent an urgent spontaneous disclosure to the FAU. Upon receiving the information, the FAU requested a freezing of these funds. The information was also sent to the Czech LEAs which resulted in immediate MLA request to country Y by the Czech prosecutor which also included a request for seizure.

553. Communication with foreign counterparts is usually carried out via Egmont Secure Web or FIU.Net. In line with the EG Principles of Information Exchange, the FAU, to the largest extent possible, provides complete, factual and legal information, which includes the analysis of the case and its potential link with the requested country. The FAU maintains the confidentiality of the information received.

Financial Supervisory Authorities

554. The supervisory authorities can exchange information with their foreign counterparts from EU and non-EU countries, including the information held by the financial institutions, this being the case only if the level of bank secrecy requirements of the requesting country complies with the Czech legislation. In practice, there was a case when supervisory authorities did not share information with the non-EU country although the requesting country claimed that its banking secrecy requirements were stronger than those in the Czech Republic and the EU.

555. The CNB cooperates intensively with its foreign counterparts and several examples of this cooperation were presented to the assessment team. The cooperation also includes on-site inspections at the requests of the foreign counterparts. Financial Market Supervision Department and Financial Market Supervision Department II are both involved in international cooperation. The examples involving the former were related to the supervision of the Czech subsidiary of the Raiffeisenbank, this being a part of the overall on-site supervision of the Raiffeisen International.

Other examples concerned cooperation with the New York Department of Financial Services and the Bank of Russia. The CNB's Financial Market Supervision Department II receives information concerning the entities supervised by the CNB at the request of its foreign partners (reference was made to 6 such cases). The information provided by the CNB was analysed and the authorities were informed about the conclusions of this analysis. In one of these cases, the CNB was not allowed to share information at the level of detail requested by the authorities, since the certain conditions required by the Czech law were not met.

556. The Financial Market Supervision Department II informs the foreign supervisory authorities about their plan of on-site inspections which concerns the agents of entities supervised by these authorities.

557. As far as the DNFBPs supervisors are concerned, no examples of such cooperation were presented to the assessment team.

International exchange of basic and beneficial ownership information of legal persons and arrangements

558. Czech authorities indicate that they have provided cooperation, via MLA, regarding beneficial ownership of legal persons and arrangements within a reasonable time period. Such cooperation will presumably be more and more prompt as the newly created Czech Beneficial Ownership Register is adequately populated. Meanwhile, the FAU manages to collect such information from other sources which are directly accessible to them.

559. Information on legal persons and arrangements is available in the Public Register, which is administrated by the Ministry of Justice. Via FAU or LEAs foreign authorities are provided access to the Public Register for which details are provided in IO.5.

Conclusions

560. Czech authorities have the means to provide and have provided cooperation on a timely basis in relation to ML matters and the requisite predicates via MLA and between other relevant authorities, particularly the FAU. This cooperation included assistance in relation to tracing, freezing, seizing and confiscation of assets. Significantly, the feedback provided in relation to the quality and constructive nature of the CzR's assistance was overwhelmingly positive. In terms of outgoing requests more detailed data with respect to underlying offences relating to ML requests might better demonstrate that all appropriate efforts were made to obtain assistance in relation to the high risk offences identified in the NRA. **The Czech Republic has achieved a level of substantial effectiveness for IO2.**

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

2. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2011. This report is available from https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680715f78.

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

1. Since this Recommendation was added in 2012, there has been no been no previous assessment of the Czech Republic in this regard.

2. *Criterion 1.1* – During the years 2015 and 2016, the Czech Republic, carried out a national ML/FT risk assessment which encompassed identification, assessment of ML/FT risks and included either suggestions, concrete proposals or action aiming at mitigation of identified risks. The assessment was led by the FAU and risks were considered in all three components: threats, vulnerabilities and consequences, though there was perhaps less emphasis on the third component in the NRA report. The authorities saw fit to put forward proposals in light of measures already in place, therefore they consider a NRA chapter which summarises the risks, description of measure for their mitigation, institution(s) responsible for its implementation including the indicative deadline for its completion as an action plan.

3. *Criterion 1.2* – The CzR has designated an authority to co-ordinate risk-assessment. The FAU has been officially confirmed in this role via S. 30a of the AML/CFT Act (referred to as "the Office"). The AML/CFT Act also creates a mechanism for the NRA, in the sense that it provides that other key government agencies and obliged entities "shall participate" in the process. S. 30a (4) provides that the NRA "shall be kept up to date".

4. *Criterion 1.3* – As mentioned above Section 30a of the AML/CFT Act mandates that the FAU and the relevant stakeholders are to keep the NRA up to date. The CzR authorities, in particular the FAU or "Office" responsible for the NRA process and, therefore, keeping it current, are projecting a refreshed version of the NRA to be put before the Government for January 1, 2021. Whilst a 4-year period may appear long, the authorities advised that in the meantime the follow-up process would be carried out targeting primarily proper distribution and awareness of the NRA reports (public and confidential versions), outreach concerning NRA results; ensuring the application of the mitigating measures as foreseen by the action plan; in addition, the authorities advised that the Government explicitly stated that different parts of NRA could be updated in case the circumstance changed and the risk evolved.

5. *Criterion 1.4* – Section 30a of the AML/CFT Act provides that the listed stakeholders "shall participate" in the NRA process. Agencies and obliged entities were also given feedback and guidance in the course of the NRA process. FAU has updated and disseminated some of its Instructions in given areas taking into account risk areas identified in the NRA and improvements made that have an impact on either all or more specific agencies or private sector participants. Large number of measures meant to mitigate risks were proposed or put in place and the relevant participants appear

to have been made aware of them. The NRA (a public version) and other information have been made available via the FAU's website. This also includes information/guidance how to use the confidential part of the NRA which was distributed to all authorities involved in the process. In addition, Czech authorities advised that twelve tailor made sector NRAs were also prepared and shared with the obliged entities concerned.

6. *Criterion 1.5* – The NRA process did have the goal of addressing specific areas and criminal phenomena of high risk and a number of measures were proposed and/or applied, including the creation of or plans for various registries such as the PRA, the registry of legal persons and trusts and the bank account registry. Plans for e.g. strengthening the requirements allowing for the gathering and updating of beneficial ownership information are a very positive development in direct response to the identification of areas presenting greater risks. The process has not yet covered all relevant areas.

7. *Criterion 1.6* – Czech Republic has not taken a decision to disapply any of the FATF Recommendations requiring FIs or DNFBPs to take actions.

8. *Criterion 1.7* – The Czech Republic has identified higher risks. Appendix No 1 to the AML/CFT Act contains non-exhaustive list of factors and types of evidence of potentially higher risk. This list includes customer risk factors, product, service, transaction or delivery channel risk factors as well as geographical risk factors.

9. According to Section 21a (1) (Risk Assessment) of AML/CFT Act the obliged entities are required to identify and assess the risks of legitimisation of proceeds of crime and financing of terrorism that can occur within their activities portfolio and which are subjects to the AML/CFT Act. While assessing the risks, the obliged entity shall also take into consideration the factors of potential higher risk stipulated in the afore-mentioned Appendix No.1 to the AML/CFT Act. The obligation for some DNFBPs to complete risk assessment, as established in the AML/CFT Act, does not require them to have such assessment in written form. However, there is no requirement for FIs and DNFBPs to take enhanced measures to manage and mitigate the higher risks identified in the NRA or to incorporate information on those risks into their risk assessments.

10. *Criterion 1.8* – Section 13 of the AML/CFT Act provides that the obliged entities may perform a simplified identification and customer due diligence in relation to categories of customers where potentially lower level of risk with regard to possible legitimisation of proceeds of crime or financing of terrorism' appears to be present. The criteria/type of product/business relationship to which the simplified identification and customer due diligence can be applied are provided in Section 13 (2) of the AML/CFT Act.

11. The simplified identification and customer due diligence shall not be applied for a customer who is a politically exposed person and for other client(s) or situation(s) of higher risk. The lower risk nature of the situation identified by the AML/CFT Act is not fully supported by the NRA findings. Meanwhile, the FAU published the risk factors identified through the NRA on its website. These factors should be taken into consideration when an obliged entity prepares its own risk assessment and revise its system of internal rules which cover also the scope of possibilities to apply the simplified CDD.

12. *Criterion 1.9* – All obliged entities have the obligation to identify and assess the risks of legitimisation of proceeds of crime and financing of terrorism that can occur within their sphere of activity (Section 21a of the AML/CFT Act). The supervisory authorities are obliged to control and monitor the implementation of the AML/CFT requirements including the risk based approach. However, the requirement to elaborate a written assessment document applies only to credit and

financial institution, gambling providers, real estate services while TCSPs (auditors, tax advisors, accountants, court bailiffs and notaries) do not have the obligation to produce the assessment in a written form. Therefore, their SRBs have limited ability to actually verify whether the AML/CFT measures undertaken by such entities are risk-based.

13. *Criterion 1.10* – Section 21a of the AML/CFT Act requires the obliged entities listed in Section 2 par.1 letters a) to d) and h) to document their own risk assessment. (a) As described under c. 1.9, the requirement does not apply to auditors, tax advisors, accountants, court bailiffs and notaries. (b) While assessing the risks, the obliged entities shall take into consideration the risk factors stipulated in the Appendix to the AML/CFT Act which contains non-exhaustive list of factors. However, as described in c. 1.7, the obliged entities are not bound to take enhanced measures based on the risks identified in the NRA or to incorporate information on those risks into their risk assessments. c) The obliged entities are required to update the risk assessment regularly, in particular prior to releasing any new product. d) The obliged entities which are required to prepare the risk assessment in a written form, have to include this document in their system of internal procedures (Section 21(2) of the AML/CFT Act). The internal procedures package is then sent regularly to the supervisor (Section 21(6 and 7) of the AML/CFT Act).

14. *Criterion 1.11* – a) According to Section 21 of the AML/CFT Act, the obliged entities shall introduce and apply adequate strategies and procedures for internal control to mitigate and manage the risks of legitimisation identified (as per Section 21a). The internal rules shall be approved by the statutory body of the obliged entity.

b) There is no explicit requirement in AML/CFT Act regarding the monitoring the effectiveness of the system of internal rules and risks mitigation measures. However, Art. 8 of the CNB Decree 281/2008 requires FIs to prepare once a year an assessment report which shall include the analysis of the effectiveness of AML/CFT procedures, potential deficiencies in their AML/CFT procedures, resulting risks and mitigating measures to remedy these deficiencies. The report has to be reasoned and approved by the statutory body. The DNFBPs remain uncovered for this element of c. 1.11.

c) Decree on certain requirements for the system of internal principles, procedures and control measures against money laundering and terrorist financing elaborates the requirements for implementation and application of: i*)procedures for the vetting of customers and setting the scope of vetting commensurate with the risk of money laundering and terrorist financing depending on the type of customer, the business relationship, the product or the transaction*, and ii) *methods and procedures for risk assessment, risk management, internal control and checks of compliance with the obligations stipulated by law, applied within the system of internal principles, procedures and control measures by entities which are subject to supervision by the Czech National Bank.* The DNFBPs remain uncovered for this element of c. 1.11 c).

15. *Criterion 1.12* – According to the Section 13 (1) and 13 (3) of the AML/CFT Act the simplified due diligence is allowed in relation to customers' categories with potential lower level of *risk with regard to possible legitimisation of proceeds of crime or financing of terrorism* and only in case there is *no suspicion* that the customer, the product/service bear any ML/FT related risk. In case of any doubt, the simplified identification and customer due diligence should not be applied. The AML/CFT regime does not fully cover criteria 1.9 to 1.11.

Weighting and Conclusion

16. Czech Republic has carried out its ML/FT risk assessment in 2016, whilst the NRA report was officially approved by the Government in January 2016. Still there are certain shortcomings such as absence of the requirement for a written risk assessment by certain DNFBPs, which limits

supervisory authorities' ability to verify whether the AML/CFT measures they have undertaken are risk-based. Moreover, there is no requirement for FIs and DNFBPs to take enhanced measures to manage and mitigate the higher risks identified in the NRA whilst certain DNFBPs are also not specifically targeted by requirements set forth in criterion 1.11. **Czech Republic is Largely Compliant (LC) with R.1.**

Recommendation 2 - National Cooperation and Coordination

17. In the 2006 MER (3rd evaluation round), former R. 31 was rated PC, as there was found to insufficient coordinated and concerted policy and other measures. In the 4th Follow-up report (2011), the rating was raised to LC based on the designation of the FAU as the authority responsible for coordination and demonstrated focus on establishing coordination between relevant agencies.

18. *Criterion 2.1* – Because of the structure of the NRA (the assessment of risks was to a large extent focussed on a patchwork of specific areas e.g., the low number of convictions for ML, the risks presented by phishing, the risks and vulnerabilities of NPOs), there were few general policies clearly articulated and summed up, though the parallel National Security Audit did formulate broad policies. There were, however, in the form of numerous measures (80 in total) proposed, certain targeted policies or concerns stated or implicit in the concrete measures proposed or put in place.

19. *Criterion 2.2* – The FAU is the central body responsible for the AML/CFT policy in the Czech Republic (Section 30a of the AML/CFT Act). Given its FIU role, the FAU appears to be well-positioned to take account of its consultation with all stakeholders (public and private) in the course of preparing proposals for AML/CFT legislation. It also provides guidance and clarification on AML/CFT legislation and advice on risks.

20. *Criterion 2.3* – CzR authorities advised that there are several inter-institutional agreements, for instance between the FAU and CNB, Police, Customs Authorities, Tax Authorities, National Security Office, Bailiff Chamber, creating an open channel of communication. There are also specific platforms preparing strategic documents identifying potential issues and areas for improvement, including one established by the Office of the Government dealing with Corruption, an identified important predicate for ML, and one by the Ministry of Interior regarding national security. In sum, there appear to be some appropriate structures and channels for the purposes of AML/CFT cooperation on the operational level and to some extent in relation to policy development. Although formally established networks are not specifically required by the standard, the absence of clear structures, including regularly scheduled contacts, linking the FAU as coordinator and the relevant agencies and private sector stakeholders, as opposed to sporadic or *ad hoc* contacts, prevents the assessors from forming a comprehensive picture of all of the relevant mechanisms.

21. *Criterion 2.4* – CzR authorities take the position that combating financing of proliferation is an integral part of the implementation of international sanctions. Authorities state that Act No. 2/1969 Coll, Section 4, par.1, that the Ministry of Finance is responsible for "*domestic coordination while implementing international sanctions for the purpose of maintaining international peace and security…and the fight against terrorism*". They add, however that, *de facto*, this obligation is taken on by the FAU. The coordination and cooperation among relevant authorities is also ensured through their participation in the inter-institutional working group. However, this group has no clear terms of reference nor does any legislation clearly set out its mandate. Their meetings are on ad hoc basis and its decisions/statements/opinions appear not to be always distributed among those concerned by these decisions.

22. Though there appears to be no clear legislative or regulatory designation in this regard, the FAU states that it is the main competent authority responsible for the coordination of the implementation of international sanctions. There is also some ambiguity as to the MFA's statutory responsibility for policy decisions and for the listing and de-listing procedures. In order to deal with the types of restrictive measures involving various stakeholders responsible for their direct implementation a specific informal working group has been formed, but the frequency and nature of the contacts between the relevant participants in this group are unclear. The FAU apparently provides *ad hoc* clarifications (via telephone consultations and some written material) to exporters about what to consider prior to the exportation of goods. The Czech Republic maintains that it fully implements all UN and EU regimes, incl. UNSCR 1540 (2004) and all sanctions imposed against Iran and North Korea. While there appear to be some channels and loose structures allowing for domestic coordination in relation to PF, there is ambiguity about the formal designation and authorization in law or regulation as to the agency or agencies responsible for the coordination of PF related issues.

Weighting and Conclusion

23. While the NRA has generated specific recommendations to deal with precise challenges and while there are some structures ensuring consequent coordination, the completeness of such structures has not been entirely demonstrated. For example, concerning PF, the ambiguity regarding a legal designation authorising one or more specific agencies as responsible for policy and operations is a shortcoming. **Czech Republic is Partially Compliant (PC) with R.2**.

Recommendation 3 - Money laundering offence

24. In the 2006 MER (3rd evaluation round), CzR was rated PC in relation to this Recommendation. In the Report on the 4th Assessment Visit (2011), a number of improvements were noted but there remained concern about the adequate criminalisation of ML. The assessors found that there was a serious deficiency relating to criminal liability for legal persons. There has since been a significant improvement in this regard. Most of the legislative improvements have been made in the "new" Criminal Code (Law No. 40/2009 Coll.) which came into force on January 1st, 2010.

25. *Criterion 3.1* –

26. In order to assess coverage of all of the aspects referred to the Palermo Convention, one must consider, according to Czech authorities, a number of different provisions under the law. First, the core offence of ML is essentially covered under S. 216-217 of the Criminal Code which renders criminally liable a person who conceals the origin or otherwise attempts to substantially complicate or render impossible to establish the origin of a*) things acquired by a criminal offense committed in the Czech Republic or abroad, or as a reward for such a criminal offense, or b) things obtained for a thing referred to in Paragraph a), or whoever allowed another person to commit such an act or conspired to commit such an act, will be sentenced to imprisonment for up to four years, to a pecuniary penalty, to prohibition of certain activity, or to confiscation of items however, if he commits such an act in relation to a thing derived from a criminal offense for which the law stipulates a lighter punishment, he will be sentenced to this lighter punishment.*

27. Participation under S. 214-215 of the CC offers further coverage of the acts specified in the Palermo Convention. An additional provision, S. 217, criminalises certain aspects of ML in relation to items of "larger value" on the basis of the lesser standard of negligence, thereby going beyond the usual FATF standard *per se*.

28. According to CzR authorities, although the specific acts and other features referred to in the Palermo Convention, Article 6 (1(a)(i) and (ii)) do not explicitly appear in the text of the CC S. 216,

the doctrinal sources of interpretation appear to support a very broad interpretation of the words "conceal the origins" contained in the first line of S. 216. More importantly, recent case law[77] provides additional arguments in this regard. While it is noted that the concept of "res judicata" does not apply *per se* under Czech law, it appears likely that the case law supporting a broad interpretation will not easily be departed from.

29. The assessors accept the Czech authorities' proposition that S. 366 ("favouritism") generally covers the second purpose referred to in the Palermo Convention Art. 6 (1 (a)), i.e., helping the predicate offender to evade the consequences of his or her action. Regarding the aspects of the Art. 6 (1 (b)), the assessors find that "acquisition", is covered through the words "transfers to himself" and "uses". As for "possession", the assessors are unable to conclude that mere possession is in fact covered, though this deficiency is considered minor.

30. *Criterion 3.2* – The CzR has adopted an "all crimes" approach, which means that all crimes are a predicate for ML. Thus the amendment of the standard in 2012 to include tax crimes has no negative effect in terms of the coverage of "a range of offences in all of the designated categories".

31. *Criterion 3.3* – The CzR does not apply a threshold approach.

32. *Criterion 3.4* – Authorities advise that a "thing" is defined in Section 134 of the CC. This definition was adapted to a new terminology of the Civil Code (Act No. 89/2012 Coll.) and was introduced through the amendment to the CC (No. 86/2015 Coll. from June 2015). The CC now applies the same definition of the term "a thing" as provided in Sections 489 - 498 of the Civil Code. This definition appears broad enough ('*a thing is everything that is different from a person and serves the needs of people'*) whilst "things" may be divided into corporeal and incorporeal (Section 496 of the Civil Code) or into immovable and movable (Section 498). Things acquired directly or indirectly from crime are covered (see par.27 above).

33. *Criterion 3.5* – It appears clear that a conviction on the predicate offence is not required to prove that given property is the proceeds of crime. The authorities advised that the judgement of Supreme Court No. 11 No. 652/2008 confirmed that the assessment of whether an asset had been acquired by a criminal act is, or may be a preliminary matter regulated by Section 9 (1) of the Criminal Procedure Code. This assessment depends on the evaluation of the circumstances of the case and a conclusion on whether a criminal act was committed. Consequently, conviction for a predicate offence is not a pre-condition for determining if ML was committed.

34. *Criterion 3.6* – S.216 of the CC specifically refers to proceeds as: "*items acquired by a criminal offense committed in the Czech Republic or abroad, or as a reward for such a criminal offense, or similarly*". S. 214 of the CC states as follows: "*an item acquired by a criminal offense committed in the Czech Republic or abroad by another person or as a reward for such criminal offense…*"

35. *Criterion 3.7* – As noted above in relation to criterion 3.6, Section 216 of the CC (with an amendment removing the words "by another person") is broad enough to capture self-laundering. Thus the principle component of the offence complies with this criterion. However, the words "by another person" still appear in S. 214 of the CC (Participation), making this provision inapplicable for the purposes of self-laundering. The same is true, to the extent that "Favouritism" (S. 366) applies in relation to one of the purposes of the act deemed to be ML, in that it refers to "assisting another person".

[77] i.e. case "7 TDO 1463/2012"

36. *Criterion 3.8* – Though Czech law does not explicitly provide that the mental element of the offence may be proved based on objective circumstances, it appears to be implicit in the language of the CPC - Article 2(6).

37. *Criterion 3.9* – Under Czech law various sanctions apply to individuals and legal persons for ML. For natural persons, the principal provision relating to ML, provides a range of up to 4 years imprisonment and other alternative sanctions (S. 216 of the CC). The range increases to 6 months to 5 years if the offence is committed in relation to an item of "larger value" and 3 to 8 years when dealing with an item of "extensive value". For participation, the same 4 categories apply. As for negligent ML or negligent participation, the ranges start with a maximum of 1 year and progress to maximum 3 years (when the offender gains a "substantial profit") and 5 years when the item is derived from an "especially serious felony". Finally, for the offence of "Favouritism" under CC S. 366, the range is up to 4 years.

38. Sanctions are generally in a serious range for the main ML offence, but certain provisions provide (for both ML and negligent ML) that where the predicate is punished at a lower level, the ML related to such predicates will be punished at this lesser level, which may fall to one year. There are also value thresholds that apply, e.g. in S. 216 of the CC - "extensive value" and for S. 214 - "greater value". These are given a numerical value in S. 138 of the CC. For "Favouritism" there is a possible exemption for "close persons" unless this offence is committed in relation to such underlying offences as Terrorist Financing or for profit.

39. *Criterion 3.10* – Act No. 418/2011 Coll. on Criminal Liability of Legal Persons and Proceedings against them includes 48 sections dealing with i) the liability of legal entities (S. 7-9); ii) the operation of such liability territorially or regarding extraterritorial acts (S. 2-5); iii) the respective and joint liability of natural and legal persons (S. 8-9); iv) the various sanctions that may be imposed including a monetary penalty (daily rate ranging from 1000 CZK to 2 000 000 CZK/EUR 38.779 to EUR 77,558), confiscation or items and property, prohibition from performing certain activities or from receiving government contracts (S. 15-23); and other matters.

40. Section 9(3) of this Act explicitly provides that criminal liability of natural and legal persons are independent of each other and may be applied in parallel, i.e., that sanctions may be imposed in relation to the same pattern of conduct not only on legal persons but also on individual members of this legal person if they both commit ML offences regardless of their involvement within legal person. A legal person may also commit an ML offence as an accomplice (Section 9 (3)). The broad range of possible sanctions against legal persons would provide the basis for proportionate, effective and dissuasive sanctions to be imposed in a given case.

41. *Criterion 3.11* – Participation in the ML offence is criminalised pursuant to the CC Sections related to ML offences (214 – 217 and 366) in connection with Section 24 of the CC. A participant in a completed offence or an attempt to commit an offence may be an organiser, an instigator or an accessory. Conspiracy to commit a criminal offence of participation (Section 214 of the CC) as well as legalisation of proceeds from crime (Section 216 of the CC) was put on par in terms of sentence with a completed criminal offence on the basis of amendment to CC No. 165/2015 Coll. An attempt to commit the ML offence is criminalised pursuant to the CC Sections related to ML offences (214 – 217 and 366) in connection with Section 21 of the CC. Aiding and abetting is punishable also under provisions related to ML offences in the CC (S.214 – 217 and 366) in connection with Section 24 (1) b) and c). Facilitating is criminalised by virtue of the provisions related to ML offences (Sections 214 – 217 and 366 of the CC) in connection with Section 24 (1) c). Counselling is criminalised by virtue of Sections 214 – 217 and 366 of the CC in connection with Section 24 (1) c).

Weighting and Conclusion

42. The CzR has made significant progress regarding many aspects of this Recommendation, most notably the advent of criminal liability for legal persons and coverage under Criterion 3.6. Although the core acts that are to be criminalised in line with the Palermo convention are not covered explicitly and perhaps not entirely, the law of the Czech Republic, when taken as a whole and in view of the recent jurisprudence provided to the assessors, appears to be sufficient to meet the essential requirements of R.3. Self-laundering is only partly covered. **The Czech Republic is LC with R.3**.

Recommendation 4 - Confiscation and provisional measures

43. In the MER 2011, Czech Republic was rated partially compliant in relation to confiscation and provisional measures under R.3 of the then FATF Recommendations, based on the factor that the confiscation of property that had been laundered was not explicitly addressed by the law as well as some effectiveness concerns and the lack of statistics on confiscation. Since then, the Czech Republic has adopted new legislation - the Law on Enforcement of Seizure of Assets and Items in Criminal Proceedings and Related Acts and significant amendments to the Criminal Code have been made.

44. *Criterion 4.1* – a) The application of confiscation is regulated by the CC (section 66, 67, 70, 71, 101, 102, 102a, 103).. Although the amended CC makes distinction between "proceeds of crime", "instrument of crime" and "substitute value" (Sections 71 and 102 of the CC), it still does not explicitly distinguish between "property laundered" and "proceeds of crime". The authorities clarified that the "property laundered" falls under the definition of "proceeds of crime" under the Section 77b of the CPC ("*asset that has been obtained through a crime or as a reward for it or has been acquired, even partially, for assets either obtained through crime or representing a reward for crime, including foetus and benefits (hereafter "proceeds of crime")".* The assessment team agrees with the reasoning provided by the authorities given the definition of the proceeds of crime which appears broad enough to cover the property laundered.

b) The confiscation of proceeds of crime is mandatory (Section 70 of the CC). Forfeiture and confiscation of an asset also affects fruits and revenues (Sections 70 and 101 of the CC) which are owned by the offender or by a person, whose asset is being forfeited. Confiscation of instrumentalities is covered by Article 70 (2) of the CC. Furthermore, on the basis of Article 102a of the CC, the court may impose forfeiture of a portion of assets.

c) S.79 a-g of the CPC designate terrorism and FT as predicate offences in relation to which proceeds and instrumentalities are subject to confiscation.

d) Sections 71 and 102 of the Criminal Code allow the confiscation of the property of equivalent value if *the offender, destroys, damages or otherwise disvalues, alienates, renders useless, removes or utilizes, in particular consumes or otherwise circumvents confiscation of such item, or if he obstructs the execution of confiscation of the item before the court.*

45. *Criterion 4.2* – a) The authorities which are competent in the area of identifying and tracing property that is subject to confiscation are police and prosecutors (for pre-trial proceedings) and the presiding judge (for court proceedings). These authorities can demand from the person whose assets are to be seized, or a person close to such a person, a statement of assets in order to ascertain the nature, extent or location of items for the purpose of their seizure, to ascertain the property of the accused or for the purpose of securing the execution of a criminal sanction (Section 7a of the CPC). Additionally, the public prosecutor (and the presiding judge after filing an indictment or a motion for punishment) may request information subject to banking secrecy and data from the register of instruments and booked securities (Section 8 CPC). During the criminal proceedings, public

prosecutor (and the presiding judge after filing an indictment or motion for punishment) may request tax information from the tax administration authority.

b) Section 79a CPC regulates the seizure of instruments and proceeds of crime by the presiding judge or (in pre-trial proceedings) the public prosecutor or police authority (the latter being possible upon previous consent of the prosecutor). This consent is not necessary if the seizure needs to be executed urgently, however the police authority is obligated to present its decision to the public prosecutor, who will then, within 48 hours, either grant it or repeal it. In addition, in case it is impossible to seize an instrument(s) or proceed(s) from crime, a property of an equivalent value may be seized. (Section 79g of the CPC).

The AML/CFT Act provides for the suspension of transactions if there is a suspicion that it could thwart or significantly hinder the seizure of proceeds of crime or funds determined for financing of terrorism for a maximum period of 3 working days (Section 20(3,b)). The FAU reports the suspension or seizure of transaction to LEA which then decides on further measures to be taken.

c) As per s.102 a of the CC, courts may impose forfeiture of assets if the offender transferred them to: i) another person free of charge or under markedly advantageous conditions and such person was aware or should have been aware that such item was transferred to them in order to avoid forfeiture of the item, or that such item was acquired contrary to the law; ii) close person, iii) legal entity, in which the offender has a majority share or majority voting right or decisive influence on the management either by himself or in connection with other close persons, and the offender uses such item either free of charge or under markedly advantageous conditions, iv) trust fund, or v) acquired to community property

The Czech Republic also introduced a specific form of confiscation in the administrative procedure regulated by the Article 167 para. 1 of Tax Code No. 280/2009 and Article 103 of Value Added Tax Act No. 235/2004. In line with these provisions, the tax administrator may issue a hedging order for tax not yet determined only if there are objective factors that give rise to a grounded concern (i.e. a reasonable ground) that (i) the tax will be determined at a certain amount in the future, and (ii) at the time of its enforceability, this tax will be irrecoverable (for example, the entity transfers assets, dampens economic activity), or its recovery will be associated with considerable difficulties. In addition to these measures, the introduction of the duty to declare a property (as per the CPC Section 7a) by a person under investigation and persons close to him/her could be, to some extent, considered as a measure relevant to this criterion.

d) The CPC provides numerous tools and mechanisms to enable seizing, freezing and confiscations of proceeds of crime. These are: Section 8 (possibility to lift the bank secrecy and obtain information from the register of investment tools and 'dematerialised and immobilised' securities, upon request of investigative authorities; monitoring of bank account or monitoring of an account of a person authorised to register investment tools and 'dematerialised and immobilised' securities; to obtain information from tax administration concerning a decision on income tax assessment). In addition, different types of special investigative means (CPC - controlled delivery (Section 86), interception and recording of communication (Section 88), simulated transfers (Section 158c), surveillance of persons and objects (Section 158d), use of undercover agents (Section 158e) are available for almost all premeditated crimes whilst some of these measures (e.g. use of undercover agents) require the maximum of a sentence of eight years and more. These measures can be used in identifying property liable to seizure, freezing and confiscation).

46. *Criterion 4.3* – The rights of bona fide third parties are protected by S. 102a paragraph 4 of the CC. In addition, Section 77b paragraph 5 of the CPC states that unless the law stipulates otherwise,

the rights of third parties to the seized item important for criminal proceedings may be asserted in civil-law proceedings.

47. *Criterion 4.4* – The Asset Management Office, which is a specialised department of the Ministry of the Interior established on 01/01/2017, manages seized movable assets. It is also in charge of setting up standards related to seized assets stored by the Police in its warehouses.

48. The sale of movable assets is based on Act No. 279/2003 Coll. (with its amendment Act No. 86/2015) on the enforcement of seizure of assets and items in criminal proceedings.

49. The Office of Government Representation in Property Affairs (OGRPA) is the authority disposing of confiscated assets (both movable and immovable) and is in charge of selling them.

Weighting and Conclusion

50. **Czech Republic is Compliant (C) with R.4**.

Recommendation 5 – Terrorist Financing Offence

51. In the 4th evaluation round (2011), the CzR was rated PC in relation to (former) SR II. The offence of terrorist attack did not adequately cover the all the acts described in Annex to the Terrorist Financing Convention. In addition, the collection of funds was not adequately criminalised whilst different provisions that criminalise FT were not adequately harmonised. Also there was no explicit indication that the offence is prosecutable without the funds being used or linked to a specific terrorist act. In the course of the follow-up process, former CC S. 95 had been replaced by a new S. 311, but there was still no stand-alone offence of FT. With the coming into force on February 1, 2017 of No. 455/2016 Coll., a new free-standing FT provision, current S. 312d was brought into force to deal more effectively with this activity.

52. *Criterion 5.1* – The International Convention for the Suppression of the Financing of Terrorism (CFT) entered into force for the Czech Republic on 26 January 2006 pursuant to its Article 26 (2). The Czech authorities provided the assessors with a comprehensive chart showing that all of the offences referred to in Art. 2, par.1 (a) are indeed covered under the CC.

53. The CFT convention, at Art. 2 par.1. (b), requires that countries criminalize FT on the basis of both intention and "knowledge" as the *mens rea* or mental element. While intention is dealt with explicitly and adequately in the text of s. 312d, the knowledge element is not referred to explicitly. Czech authorities indicate, however, that this element is captured by means of the general principles of criminal liability under Czech law, codified under s. 15 of the CC, which has - an intentional element - both *dolus directus* (s. 15(1)a)) and *dolus eventualis* (s. 15(1)b) and (2)). The latter is such that a person may be convicted of the an offence (including FT under s. 312d) based on evidence that he/she was aware in a general way that his/her conduct "may" violate or endanger an interest protected by the CC and that he/she understood it.

54. While S. 312d covers the financing "directly or indirectly" through the words "himself or through another person", the funds or property "in full or in part" being destined for use by terrorists or in the commission of terrorist offences is not explicit. In the explanatory report to Act. No. 455/2016, the legislator makes clear his intention to cover both "in full" and "in part" and that the general rules of interpretation of the Criminal Code tend to support a broad coverage unless a contrary intention appears from a reading of the relevant provision. However, the explanatory note, while it may have a strong influence on a judge, is not technically binding in law.

55. *Criterion 5.2* – Section 312d refers in par.1 to a person who supports a terrorist group, its member, a terrorist, or the commission of [various offences] or collects finances or other items "with

the intent to use them in this manner…". The formulation in the English language translation leaves something to be desired in terms of clarity, but based on discussions with the Czech authorities, the assessment team accepts that the Czech version of the relevant sentence should be read as "… collects finances or other items with the intention that they be used in such a [terrorist-related] way" and as such meets the requirements of this criterion. The new provision seems broad enough to cover FT "for any purpose", as the support in the first group of intended recipients refers to a terrorist group, a member of one, or a single terrorist without reference to a purpose. Although "materially supports" is not explicitly defined, CzR authorities refer to the words of the provision dealing with the aspect of collection - "*collects finances or other items (things)"* and advised that to understand the term "thing" one must look to the very broad definition found at S. 489, 496, 498 of the Czech Civil Code (already elaborated under R.3). Therefore, the FATF definition of "funds" would appear to be entirely covered, since the net effect of the relevant Civil Code provisions is to cover any property, essentially.

56. Although there are a number of requirements for a group to be considered a "Terrorist Group" under the CC S. 129a, including a minimum of 3 "criminally liable individuals" a "permanent" nature, a division of activities and using planning and coordination aimed at the commission of terrorist offences, these features would generally be present in most terrorist groupings. However, S.312d covers an individual terrorist ("terrorist group, its member, a terrorist") and financing two individual terrorist would then be covered.

57. *Criterion* 5.2 *bis* – S. 312d of the CC refers to the offences in S. 312e as part of FT. S. 312e (2) (b) and (c) of the CC criminalise providing or receiving terrorist training. S.312e(3) refers to the offences in 312e (2)(b) and (c) and criminalises travelling for this purpose together with traveling for the purpose of committing participation in a terrorist group (S. 312a), threat by terrorist criminal act (S. 312f) or a criminal offense referred to in 312e sub-section 2 (b) or c). This adequately covers the requirements of 5.2 *bis*.

58. *Criterion 5.3* – The authorities take the view that, since the law does not distinguish or limit the types of support that may be the subject of a prosecution/conviction based on S. 312d, it can be assumed that the law simply does not differentiate between legally and illegally obtained funds or material support that is made available to terrorists. Support for this view is found in the explanatory report to Act No. 455/2016 and in case law dealing with respect to support provided to organised crime under CC s. 361.

59. *Criterion 5.4* – It is not clear on first reading of English translation of the CC whether S. 312d meets all the requirements of this criterion. Whilst the exact wording at first glance appears incomplete, as mentioned in relation to criterion 5.2, the assessment team was convinced that the problem lay in the translation, rather than the original Czech language text of the provision. As previously noted in relation to C.5.2 above, S. 312d does properly break the link, as required, between the financing and a terrorist act in the first line of the provision.

60. *Criterion 5.5* – As discussed in relation to C.3.8 above, and on the same grounds, this criterion is met.

61. *Criterion 5.6* – Under S. 312d, the lowest range of sentence is imprisonment for a term between 3 and 12 years, whereas in the presence of certain aggravating factors (if a member of an organised group, if in time of national peril or war, if FT on a greater scale), the range may be increased to 5-15 years based on the circumstances of the commission of the offence listed in 312d(2)a),b),c) (precisely what constitutes "to a great extent" may be determined by a court having regard to the monetary value of the damage or profit, or to magnitude (e.g. multiple counts simultaneously or in

short succession). In addition, confiscation of assets may be ordered in parallel to these sentences of imprisonment. These various possible sentences appear to be proportionate and dissuasive.

62. *Criterion 5.7* – Section 7 of the Criminal Liability of Legal Persons Act lists the offences for which a legal person cannot be held criminally liable – the list does not include the criminal offence of financing of terrorism pursuant to Section 312d CC.

63. Section 9 (3) of this Act stipulates that the criminal liability of natural and legal persons are independent from each other and may be applied in parallel, meaning that the sanctions may be imposed to legal persons but also to an individual members of the legal person if he/she committed a criminal offence. Criminal liability of a legal person is not precluded by the fact that a particular natural person, acting as specified in Section 8 (1, 2) cannot be identified (Section 8 (3) of the Act).

64. Legal person may also commit a criminal offence of financing of terrorism as an accomplice (Section 9 (3) of the Act).

65. Criminal sanctions which may be imposed to a legal person for criminal offence of financing of terrorism are listed in Section 15 of the Act and they include i) dissolution of the legal entity, ii) confiscation of property, iii) fines, iv) confiscation of items, v) prohibition to perform certain activity, vi) prohibition to perform public contracts or to participate in public tenders, vii) prohibition to receive endowments (grants) and subsidies, and viii) publication of a judgement. These appear to be proportionate and dissuasive.

66. *Criterion 5.8* – For the same reasons given in 3.11, this Criterion is met.

67. *Criterion 5.9* – Because the CzR adopts an "all crimes" approach, FT is a predicate for ML.

68. *Criterion 5.10* – As opposed to the equivalent ML provision, there is no specific mention in S. 312d of the location of the FT and the terrorist act in terms of jurisdiction. Czech authorities rely on their general CC provisions (S. 4-8). In the assessors' view, particularly because of the principle of universality (S.7 of the CC), there is full coverage of this requirement.

Weighting and conclusion:

69. The CzR is to be commended for having introduced new S.312d, as it covers a number of requirements that had not been considered met by the earlier provisions, including FT "for any purpose "and the direct and indirect collection or provision of funds. The broadening of the meaning of the word "things" is also a step forward. However there are perhaps still minor deficiencies as noted in relation to C.5.1 as noted above. **The Czech Republic is LC with R.5.**

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

70. In the 2011 MER, Czech Republic was rated LC with the former SR III. There were concerns on coverage of the concept "funds and other assets" by the freezing obligation. The procedures for unfreezing the funds did not guaranty the timeliness of the process. There was a lack of guidance and training. Czech Republic implements UNSCRs 1267/1989 and 1988 and 1373 primarily through EU/EC mechanisms. The implementation of targeted financial sanctions is ensured by the Section 2 of the Act on Implementation of International Sanctions (IISA).

71. *Criterion 6.1* – Czech Republic implements targeted financial sanctions pursuant to UNSCR 1267/1988 (on Afghanistan) - through Regulation (EU) 753/2011 and Council Decision 2011/486/CFSP, and UNSCR 1267/1989 (on Al Qaida) - through Regulation (EU) 881/2002 (and successors) and Council Decision 2016/1693/CFSP (replacing the Common Position 2002/402/CFSP), which have direct effect in all EU member states.

a) The MFA would cooperate with the relevant UN Security Council Committees for proposing persons or entities for designation as the national coordinating authority, according to Part 1, Section 6 of the Act No. 2/1969 Col. of the Czech National Council "On the Establishment of Ministries and Other Central Authorities of the Czech Republic".

b) On January 23, 2018 Czech Republic established a formal mechanism for identifying targets for designation[78], based on the criteria set out in ISIL (Da'esh) and Al-Qaida (UNSCR 2368). However, these procedures do not extend to listing requirements stipulated under UNSCR 1988.

c) The "evidentiary standard" is applied in compliance with the relevant UN 1267/1989 Sanctions Committee standards, which is not conditional on existence of criminal proceedings[79].

d) Based on the internal procedure for listing under the ISIL (Da'esh) and Al-Qaida (UNSCR 2368) Sanctions Regime must be submitted via UN standard forms. These rules do not extend to listing requirements on Taliban (UNSCR 1988).

e) Proposal for designation under UNSCR 2368 should contain a detailed statement in support of the proposed listing and specific criteria. No rules are set for proposal for designation under UNSCR 1988.

72. *Criterion 6.2* – The Czech Republic implements UNSCR 1373 principally through EU Council Regulation 2580/2001 and EU Council Common Positions 2001/931/CFSP. Implementation of targeted financial sanctions is ensured by the Section 2 of the IIS Act.

a) At European level the EU Council is the competent authority for making designations according to EU Council Regulation 2580/2001 and EU Council Common Position 2001/931/CFSP. The Czech Republic has identified the MFA as the competent authority for designation of persons or entities meeting designation criteria set forth in UNSCR 1373 either at its own initiative or at the request of another country.

b) At EU level, identification of designation targets is covered by CP 2001/931/CFSP. The Czech Republic reported that it has recently established a formal mechanism for identifying targets pursuant to UNSCR 1373 at the national level.

c) At European level, the Council of Ministers is the competent authority for making EU designations under UNSCR 1373, using designation criteria consistent with those in Resolution 1373. The Working Party on restrictive measures to combat terrorism (COMET WP) uses a "reasonable basis" evidentiary standard, and designation is not conditional on the existence of criminal proceedings. At the national level, no explicit arrangement for the verification of designation requests received from third countries seem to be in place.

d) The COMET WP assesses whether the request is substantiated enough and whether it meets the designation criteria stipulated under Common Position 2001/931/CFSP. It further makes a decision on recommendation to be adopted by the EU Council, based on reliable and credible evidence, without it being conditional on the existence of an investigation or conviction (Art. 1(2) and (4)). At national level, as indicated by the country the evidentiary standard of proof would be applied when deciding whether or not to make a

[78] These procedures were formally approved on 20 April, 2018 by Deputy Minister of Foreign Affairs.
[79] Based on the Procedures for listing proposal for designation can be made not only by the LEAs, but also by the Intelligence Services.

proposal for designation. The Czech Republic further described that for the "evidentiary standard" they consider the one provided under the CPC should be applied.

e) At the European level, there is no specific mechanism that would allow for requesting non-EU member countries to implement the EU list. All EU designations must have sufficient particulars and substantiated to permit effective identification of the person to be designated, thus facilitating the exculpation of those bearing the same or similar names (Art. 1(5) of 2001/931/CFSP). At the national level, there is no formalised procedure under which the Czech Republic could ask another country, including the EU countries, to give effect to freezing measures undertaken by Czech authorities. However, the FAU is allowed to cooperate with competent foreign authorities as well as with international organisations for the purpose of fulfilment of the purpose of international sanctions (Section 14 para. 9 of the IIS Act).

73. *Criterion 6.3* –

a) At European level, all EU Member States are required to provide each other with the widest possible range of police and judicial assistance on TFS matters, inform each other of any actions taken, cooperate and supply information to the relevant UNSCs (Art. 8 Reg. 881/2002; Art. 8 Reg. 2580/2001; Art. 4 CP 2001/931/CFSP). At national level, no specific arrangement is set out to collect or solicit information to identify targets for the purpose of designation.

b) Designations at the European level take place without prior notice to the person/entity identified (EC Regulation 1286/2009 preamble para.5). The EU Court of Justice makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effect of the first freezing order. The listed person or entity has the right to appeal against the listing decision in Court, and seek to have the listing annulled. There is no further regulation at the national level related to prior notification.

74. *Criterion 6.4* – The European procedure implies a delay between the date of a designation by the UN and the date of its transposition into European law under Regulations 881/2002 and 753/2011 respectively, because of the time taken to consult between European Commission departments and translate the designation into all official EU languages. Thus, implementation of targeted financial sanctions pursuant to UNSCRs 1267/1989 and 1998, does not occur "without delay", within hours as ideally required by the FATF standards.

75. At national level, there are no formal mechanisms to implement TFS without delay, ensuring its enforceability. Under IIS Act in Section 2 "Definition" it is set out that international sanctions also include the UNSCs decision. According to Methodological Instruction 5 the Czech Republic set up a mechanism for prompt circulation by the FAU of information on entities listed in relevant UNSC, through the MoneyWeb channel. Under Section 6 of the AML/CFT Law there are provisions for the REs to consider each case as a suspicious transaction, when any transaction participant is a listed person or entity. However, none of these measures ensure implementation of the TFS in accordance with the requirements of the FATF standards.

76. Targeted financial sanctions, related to UNSCR 1373, are implemented by Council regulations (Regulation 2580/2001) that are implemented directly in Czech legal framework. These sanctions are thus implemented "without delay".

77. *Criterion 6.5* – The FAU is designated as the competent authority responsible for the implementation and enforcement of the targeted financial sanctions under the EU and national

framework, based on the provisions of the IIS Act and the AML/CFT Act. Freezing obligations have been further stipulated under MI 5.

a) In accordance with UNSCRs 1267/1988 and 1989, EU regulations establish the obligation to freeze all the funds and economic resources belonging to a person or entity designated on the European list. However, because of the delays in the transposition of UN designations, freezing action is not implemented "without delay", and this delay can actually result in prior notice to the persons or entities concerned.

   For designations under UNSCR 1373, the regulations are self-executing in all member States and no prior notice is to be given to the designated persons or entities. Listed EU "internals" are not subject to freezing measures but only to increased police and judicial cooperation among member states (CP 2001/931/CFSP footnote 1 of Annex 1). Art. 75 of the Treaty of Lisbon (2007) allows for the freezing of assets of designated EU nationals, but the EU has not yet implemented this provision. In Czech Republic, however, the freezing obligations under Regulation 2580/2001 also apply to internal terrorists designated by the EU, as stipulated under Sections 2 and 10 of IIS Act and MIs.

   At the national level the Czech Republic reported to use the AML/CFT Act before the designation under the UN TFS is transposed in the EU legal framework, and apply the IIS Act after the subjects are listed within the EU framework.

   According to Section 6 par.2 of the AML/CFT Act a transaction shall be perceived as suspicious, should:

   i) the customer or the beneficial owner be a *person* against whom the Czech Republic had imposed international sanctions under the Act on Implementation of International Sanctions,

   ii) the *goods or services* involved in the transaction fall in the category against which the Czech Republic had imposed international sanctions under the Act on Implementation of International Sanctions.

   The suspension of a client order under Section 20 of the AML/CFT Act is possible for only 3 working days and if the suspicion of FT is confirmed, the FAU submits a criminal notification to police bodies and the transaction can be suspended for a further period of 3 working days to enable the LEAs to decide on steps to be taken. This mechanism does not ensure permanent application of measures, for the duration of validity of the UN actions.

   According to a mechanism set out under Section 11 (1) and Section 12 (1)-(2) of the IIS Act should the *asset* subject to international sanctions be identified persons should not be allowed to handle it. The FAU has discretion to take a decision on application of restriction or prohibition to handle such asset within 30 days from the receipt of the report, or in a justified case may prolong the time frame. The FAU shall ensure the administration of delivered or dispossessed assets for the duration of international sanctions or until its delivery to the authorised person.

   Both mechanisms give a possibility for taking a discretionary decision for application of the freezing measures by the authorities which raises doubts about the compliance of the system with the standards.

   b) Pursuant to UNSCR 1267/1989 and 1988, the freezing obligation extends to all funds and other assets that belong to, are owned, held or controlled by a designated person or entity. The obligation to freeze the funds or assets of persons and entities acting on behalf of, or at

the direction of, designated persons or entities is covered by the notion of ''control'' in Regulations 881/2002, and 753/2011. With regard to UNSCR 1373, the freezing obligation however does not cover a sufficiently broad range of assets under the EU framework - EU Regulation 2580/2001.

According to Section 11 of the IIS Act the Czech Republic extends freezing obligation to "assets subject to international sanctions". However the definition as provided under Section 3 of the IIS Act is limited, and does not cover a sufficiently broad range of assets as given under the FATF Recommendations.

c) EU Regulations[80] prohibit EU nationals and persons within the EU making funds and other assets available to designated persons and entities. Sections 5 and 11 of IIS Act set out national framework for prohibitions, which however are not sufficiently broad to cover all requirements as provided under the FATF Recommendations.

d) The Council and the European Commission make Regulations and Decisions public through the Official Journal of the European Union, which can be accessed on the website of the European Union. Furthermore, all EU legal acts are being published in the Czech official gazette Collection of Laws (Coll.). Information for reporting entities on restrictive measures is also available on the websites of the FAU at www.financnianalytickyurad.cz, with the possibility of subscription to the newsletter. While the DNFBPs should refer to the FAU or UN websites to get updated information on designations, financial institutions receive updates from the FAU via MoneyWeb channel. Additional instructions for reporting entities are provided under FAU's MI 5.

e) Natural and legal persons (including FIs/DNFBPs) are required to provide immediately any information about accounts and amounts frozen under EU legislation per articles 5.1 of EU Regulation 881/2002, 4 of EU Regulation 2580/2001, and 8 of EU Regulation 753/2011.

At national level according to Section 10 of IIS Act, anyone finding out asset subject to international sanctions located with him should report it to the FAU without undue delay. Reporting obligation for obliged entities is stipulated under Section 18 para. 5 of the AML/CFT Act.

f) According to EU regulations (Art. 6 of 881/2002, Art. 7 of 753/2011) and AML/CFT Act (Section 24) if acting in good faith, natural or legal person, group or entity or its directors or employees shall not be held liable for freezing (suspension) of funds, other financial assets and economic resources, unless it is proved that the freezing was due to negligence. Furthermore, Section 11(5(a)) of IIS Act states that the FAU shall deliver to the authorised person the asset if it is a person which is not a subject to international sanctions and who proves to be the owner or authorised holder of that asset.

De-listing, unfreezing and providing access to frozen funds or other assets

78. *Criterion 6.6* – Czech Republic applies the following procedures for de-listing and unfreezing the funds or assets of persons and entities no longer meeting the designation criteria:

a) On 23 January 2018, the Ministry of Foreign Affairs has established[81] formal procedures for de-listing requests pursuant to UNSCR 2368, however this procedure is not publicly

[80] EU Council Regulation 881/2002 (article 2 (2)), 1286/2009 (article 1(2)), 753/2011 (article 4) and 754/2011 (article 1)

[81] Formally approved on 20 April, 2018 by Deputy Minister of Foreign Affairs.

available. Moreover, this procedure does not explicitly cover the delisting requirement under UNSCR 1988.

b) Pursuant to UNSCR 1373, the EU Council revises the list at regular intervals. Modifications to the list under Regulation 2580/2001 are self-executing. Procedure for submission of the de-listing requests is described in Criterion 6.6 (a). The Czech Republic reported that on January 23, 2018 it established a national procedure for requesting removal from the EU list. With regard to unfreezing, in addition to the EU mechanisms, the IIS Act introduced a domestic procedure under Art. 12(1(h)), according to which the FAU may decide to release assets if the international sanction has been cancelled.

c) Designated persons and entities may challenge the EU act imposing relevant sanctions by instituting proceedings (according to Art. 263, para. 4 and Art. 275, para. 2 TFEU) before the EU Court of Justice, regardless of whether the designation was initiated by the EU on its own motion, or pursuant to UN sanctions.

d) & e) With regard to designations under UNSCR 1988 and 1989, designated persons and entities are notified of their designation and the reasons, as well as its legal consequences. They have the right to request a review of the designations. At the European level, there are procedures that provide for de-listing, unfreezing funds and reviewing designation decisions by the EU Council.

At the UN level, the review can be brought before the Ombudsperson (established pursuant to UNSCR 1904 (2009)) for the examination of de-listing requests, in compliance with UNSCR 1989 and 2255, or before the UN Focal Point Mechanism (established pursuant to UNSCR 1730 (2006)) for UNSCR 1988. Interested parties may submit their requests directly to the above-mentioned EU and UN institutions.

f) EU Best Practices for the effective implementation of restrictive measures provide publicly known procedures for obtaining assistance for verifying whether persons or entities having the same or similar name as designated persons or entities (i.e. a false positive) are inadvertently affected by a freezing mechanism. However, no additional information was provided by the authorities on national procedures for unfreezing in case of false-positives.

g) De-listing and unfreezing decisions taken in accordance with EU Regulations are published in the Official Journal of the EU. Information is also published on the FAU's website and circulated to financial institutions via MoneyWeb.

79. *Criterion 6.7* – Access to frozen funds and other assets is provided under Art. 2a of EU Regulation 881/2002 and Art. 5-6 of EU Regulation 753/2011, which are directly applicable in Czech Republic. At national level such provisions are stipulated under Section 9 of the IIS Act.

Weighting and conclusion

80. The CzR to some extent meets the requirements under Recommendation 6. However, the inability to freeze without delay the assets of persons/entities designated by the UN, as well as shortcomings identified in relation to the listing and delisting procedures constitute significant deficiencies in meeting c. 6.1, 6.4 and 6.6. **Czech Republic is PC with R.6.**

Recommendation 7 – Targeted financial sanctions related to proliferation

81. Requirements under the R. 7 are first introduced in the FATF standards since 2012, and therefore, the Czech Republic was not previously assessed against these provisions. As a member of

the EU, Czech Republic applies the EU framework for implementing designations under UN Security Council Resolution 1718 (DPRK) through the Council Regulation No. 2017/1509, Council Decision 2016/849/CFSP). Security Council Resolution 1737 (Iran) is transposed into the EU legal framework through Council Regulation No. 267/2012 and Council Decision 2010/413/CFSP. Council Regulation (EU) 2015/1861 introduces changes to take account of the Joint Comprehensive Plan of Action, which apply from 16 January 2016. These Regulations have direct force of law from the date of their publication in the Official Journal of the European Union.

82. *Criterion 7.1* – Although there are delays in the transposition of UN designations into European law, the EU applies sanctions with respect to Iran to a larger number of entities that are not concerned by a UN designation, and in some cases is ahead of UN. For TFS against DPRK, the most recent additions to the UN list of sanctioned persons and entities, made through UNSCR 2270 (2016) were transposed into the applicable decision by the Council of the European Union within seven days of their designation by the UN. Delays in transposition could have therefore had some practical effect on DPRK sanctions regime in recent years. Moreover, the European procedure for prior authorisation of transactions with Iranian entities also allows authorities to refuse authorisation for any transaction with entities designated by the UN but not yet designated at the European level. As in case of Criterion 6.4 the obligations related to assets subject to international sanctions are stipulated under IIS Act and the AML/CFT Act. However, these mechanisms do not ensure enforceability of UN TFS in the Czech Republic, and therefore it cannot be understood as implementing the sanctions.

83. *Criterion 7.2* – The FAU is designated as the competent authority responsible for the implementation and enforcement of the targeted financial sanctions under the EU and national framework, based on the provisions of the IIS Act and AML/CFT Act.

a) The freezing obligation under EU Regulations is activated upon publication of the decisions and regulations in the EU Official Journal and is directly applicable to all natural persons who are EU citizens and to all legal persons established or formed under the law of a Member State or associated with a commercial transaction carried out in the EU. The delays in transposition raise the question of compliance with the obligation to execute freezing measures ''without delay'' and "without prior notice'', unless entities are previously listed by the EU.

At the national level further freezing mechanisms are set out in the Section. 6 para 2 and Section 20 of the AML/CFT Act, and Sections 11(1) and 12 (1)-(2)of the IIS Act. As indicated in Criterion 6.5 both mechanisms give a possibility for taking discretionary decisions for application of the freezing measures by the authorities. The AML/CFT Law does not ensure permanent application of measures, for duration of validity of the UN actions.

b) Under the EU framework the obligation to freeze funds extends to all types of funds or other assets as stipulated under the FATF Recommendations. According to Section 11 of the IIS Act the Czech Republic extends freezing obligation to "assets subject to international sanctions". However the definition as provided under Section 3 of the IIS Act is limited, and does not cover a sufficiently broad range of assets as given under the FATF Recommendations.

c) At European level, Regulations 329/2007 (Art. 6.4) and 267/2012 (Art.23.3) prohibit making available, directly or indirectly, funds or economic resources to designated persons or entities or for their benefit, unless otherwise authorised or notified in compliance with the relevant UN resolutions. Sections 5 and 11 of IIS Act set out national framework for prohibitions, which however are not sufficiently broad to cover all requirements as provided under the FATF Recommendations.

d) The Council and the European Commission make Regulations and Decisions public through the Official Journal of the European Union, which can be freely accessed on the website of the European Union. Furthermore, all EU legal acts are published in the Czech official gazette Collection of Laws (Coll.). Information for obliged entities on restrictive measures is also available on the websites of the FAU at www.financnianalytickyurad.cz, with the possibility of subscription to the newsletter. Furthermore, financial institutions receive updates from the FAU via MoneyWeb channel. Additional guidance is provided under FAU's MI 5.

e) At European level according to Regulations 329/2007 (Art. 10) and 267/2012 (Art. 40) obliged entities are obliged immediately provide to the competent authorities all information that will facilitate observance of the EU Regulations, including information about the frozen accounts and amounts.

At national level according to Section 10 of IIS Act, anyone finding out asset subject to international sanctions located with him should report it to the FAU without undue delay. Reporting obligation for obliged entities is stipulated under Section 18 para. 5 of the AML/CFT Act.

f)At European level the rights of bona fide third parties are protected according to provisions of Regulations 329/2007 (Art. 11) and 267/2012 (Art. 42). Furthermore, Section 11(5(a)) of the IIS Act states that the FAU shall deliver to the authorised person the asset if it is a person which is not a subject to international sanctions and who proves to be the owner or authorised holder of that asset.

84. *Criterion 7.3* – At European level Member States are required to take all necessary measures to ensure that the EU regulations on this matter are implemented and to determine a system of effective, proportionate and dissuasive sanctions in line with Regulations 329/2007 (Art. 14) and 267/2012 (Art. 47). Art. 15 of IIS Act provides that supervisory government bodies shall oversee also fulfilment of obligations under IIS Act. If there is no such government body, the supervision shall be carried out by the FAU. The CNB shall control the fulfilment of obligations under the IIS Act by persons under its supervision. Section 18 of the IIS Act further provides sanctioning measures for non-compliance with the provisions of the law.

85. *Criterion 7.4* – Czech Republic applies the following procedures for de-listing and unfreezing the funds or assets of persons and entities no longer meeting the designation criteria:

a) At European level the EU Council of Ministers communicates its designation decisions and the grounds for listing, to designated persons and entities. The latter have the right to request a review of the decision. Based on such a request or if new substantial proof is presented EU Council must reconsider its decision. Individual de-listing requests may be directly filed with the Council of the EU or with the competent UN authority (Focal Point established pursuant to UNSCR 1730 (2006)). These must be processed upon receipt, in compliance with the applicable legal instrument and EU Best Practices. Designated persons or entities are notified of the EU Council decision and can use this information to support a de-listing request filed with the UN. In addition, according to Regulations 329/2007 (Art. 13.1 (d), (e)) and 267/2012 (Art. 46) when the UN decides to de-list a person, the Commission modifies the lists in the annexes of the European regulations without the person in question having to request it. Designated persons or entities individually affected may also institute proceedings before the European Court of Justice in order to challenge the relevant (EU) Sanctions Regulations. At national level there are no formal mechanisms in place for de-listing persons and entities.

b) Procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities are provided for at an EU level. In the Czech Republic unfreezing will generally be carried out based on FAU decision. No further information was provided by the authorities on national procedures for unfreezing in case of false-positives.

c) At the EU level, there are procedures for authorising access to funds or other assets if member states' competent authorities have determined that the exemption conditions of UNSCRs 1718 and 1737 are met (Art. 7 Reg. 329/2007; Art. 26-28 Reg. 267/2012). The FAU is the competent authority for dealing with this matter, authorities of which are stipulated under Section 9 of the IIS Act.

d) De-listing and unfreezing decisions taken in accordance with EU Regulations are published by the EU and information is also published on the FAU's website and circulated to financial institutions via MoneyWeb. The Czech Republic has not developed further guidance on obligations with respect to de-listing or unfreezing actions.

86. *Criterion 7.5* –

a) The Czech Republic relies on the direct implementation of the European Regulations 329/2007 (Art. 9) and 267/2012 (Art. 29), permitting the payment of interests or other amounts to the frozen accounts, or payments due under contracts, agreements or obligations that arose prior to the date when those accounts became subject to the provisions of respective resolution, provided that the amounts are also subject to freezing measures.

b) With regard to the freezing measures pursuant to UNSCR 2231, special provisions set out in Regulation 267/2012 (Art. 24 and 25) authorise the payment of sums, due under a contract which arose prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the regulation (and de facto the UNSCR), and after prior notice is given to the UN Sanctions Committee.

Weighting and conclusion

87. The CzR meets to a certain extent a part of requirements of Recommendation 7. The inability to freeze the assets of UN designated persons without delay (albeit partly mitigated in practice by the EU framework related to Iran), lack of guidance to the obliged entities on TFS, as well as absence of delisting/unfreezing procedures constitute a significant deficiency in the system. **Czech Republic is PC with R.7.**

Recommendation 8 – Non-profit organisations

88. In the 4th round MER Czech Republic was rated partially compliant with the previous SR VIII (non-profit organisations). The MER noted that despite the efforts made by the authorities in this respect, there were still concern related to the lack of fully comprehensive review of domestic NPOs, insufficient awareness raising campaigns, training and guidance in the NPO sector, and obliged entities, regarding potentially vulnerable NPOs, non-sufficient targeted supervision or monitoring of NPOs which control significant portions of the financial resources of the sector and substantial shares of the sector's international activities. Since the previous MER, some legislative steps were taken in the country to ensure greater compliance with the FATF requirements. Namely, State Policy towards NGOs 2015-2020 was approved by Government Resolution No. 608 of 29 July 2015. Under Public Registration Act (PRA), which has been effective since 1 January, 2014 the amount of publicly available information on NPOs has been extended. Another positive aspect is the creation of the Beneficial Owner Register, which came into being on January 1, 2018.

89. *Criterion 8.1* –

a) The Czech Republic has concluded its NRA in 2016, where a separate chapter is dedicated to the analysis of NPO sector vulnerabilities. The concept of NPOs includes associations, unions, public benefit companies, institutes, religious legal persons, foundations and endowment in the CzR. For the purpose of defining the vulnerable segment of the NPOs, application of additional mitigation measures and strengthening cooperation among stakeholder agencies, a working group, with the involvement of a range of government authorities was established under the coordination of Ministry of Interior to analyse the FT risks posed by the NPO sector. The Working Group has identified the whole subset of NPOs as falling within the FATF definition due to the fact that all types of these organizations are entitled to organize public fundraising. The risk of FT exposure was identified as being high. The understanding of the risks could however further benefit from analysis based on legal form, purpose and scope of activities, other relevant features, as well as a review of the adequacy of the institutional framework for risk-based supervision of this sector.

b) The NRA has estimated the risk of NPOs exposure to FT being high. Irrespective of the fact that there have not been any actual cases of NPOs abuse for FT, the NRA provides for hypothetical examples of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs. These examples include influence of foreign actors on radicalization of individuals or respective groups transfer of foreign hazardous NPOs' activities to the Czech Republic. Some information on the scale of involvement - misuse of the NPO, recommended mitigating measures, AML/CFT prevention system, international sanctions obligations is also provided on the FAU official website. No additional typologies have been produced on abuse of NPOs for FT.

c) The authorities have conducted a review of the legislation in the course of the NRA. Legislative updates in relation to the registration, sanctioning, record-keeping and information sharing requirements have been made. Unavailability of certain information on NPOs, insufficient transparency and provability of record-keeping have been identified by the authorities as potential vulnerabilities for ML/FT. The identified shortcomings have been addressed by respective legislative amendments.

d) No specific periodicity of review of the NPO sector is specified. According to authorities the overview is to be updated according to change of the situation.

90. *Criterion 8.2* -

a) The Government Council for Non-Governmental Non-Profit Organizations (RVNNO) coordinates cooperation between ministries, other administration authorities and bodies of territorial self-governing units in the area of support for NPOs, including the subsidy policy from public budgets. It has issued "Principles of Government for provision of subsidies for NPOs from state budget". According to this document recipients of subsidies are obliged to do double-entry bookkeeping. RVNNO also issues annual review on financing of NPOs from public budget. Apart from this, there are several legal requirements that contribute to promote transparency, integrity and public confidence in the administration and management of NPOs. The CzR has made major legislative amendments in the field of transparency of NPOs and on their publicly available information. The Public Registers Act (PRA Act) was adopted in 2013 and came into full effect on 1 January 2014. According to Section 66 of PRA Act, the collection of documents includes memorandum of association of a legal person, statute of a foundation, statute of an endowment or institute, statutes of an association; decision on election or appointment, appeal or proof of another termination of a

function of persons who are members of a statutory body; annual report, regular, extraordinary and consolidated financial statements, if they are not included in the annual report. Public registers are online available at https://or.justice.cz/.

b) RVNNO is a permanent consultative, initiative and coordination body of the Government of the Czech Republic in the area of non-governmental non-profit organizations. RVNNO collates, discusses and, through its chair, submits to the government materials relating to NPOs and the creation of a suitable environment for their existence and activities. Apart from this, RVNNO, together with the FAU and MFA undertakes educational programs to raise and deepen awareness among NPOs about the potential vulnerabilities to FT abuse and FT risks. This however has not been confirmed on-site. As mentioned above, a special working group has been created to review the NPO sector, assess its potential vulnerabilities and develop mitigating measures. The working group consists of representatives of ministries and LEAs. However, the working group does not involve representatives from the NPO sector, whereas the presence of the latter would provide added value to the works undertaken by the WG.

c) Apart from this no information was provided by the authorities on cooperation between state authorities and the NPO sector in developing and refining best practices to address terrorist financing risk and vulnerabilities.

d) There is no provision under CzR legislation encouraging NPOs to conduct transactions via regulated financial channels. This is normally done by consultations with the private sector.

91. *Criterion 8.3* – Foundations, institutes and associations should obtain legal personality upon registration with the Registry courts according to the PRA Act. Religious communities can choose if they want to be registered in order to obtain legal personality or not. Registration of religious organizations is carried out by the Ministry of Culture on the basis of Act on Churches and Religious Societies and Administrative Code. Registered information is publicly accessible free of charge.

92. PRA Act provides the obligation for NPOs to provide annual reports and financial statements to the Register Court. Public benefit organizations, institutions, foundations and endowment funds must compile and publish financial statements. This obligation also applies to associations (and branch associations) and church legal persons whose income or property exceeds the statutory amount. The financial statements are published by depositing them in the collection of documents no later than 12 months after the balance sheet date of the published financial statements (Section 21a, Accounting Act and Section 66, PRA Act). Churches and Religious Societies publish an annual report on their special rights and may also publish information on their activities.

93. All NPOs irrespective of their purpose and activity, are accounting units (Section 1a of Accounting Act). An accounting unit is obliged to keep accounts in such a way that the financial statements compiled on their basis are comprehensible and provide a true and fair view of the unit's accounting and financial position. Accounting units prepare financial statements that consist of the balance sheet, profit and loss statement and attachments under Section 18 para 1 of the Accounting Act. The Tax Administration is authorised to impose fine in the case of violation of Accounting Act.

94. At the same time according to the NRA, it is stated that NPOs include religious legal persons, whereas the churches and religious organizations which have not applied for registration are not considered to be NPOs and no control measures applied in relation to them.

95. In 2016 the Czech Republic adopted the amendment of the PRA Act, which regulates Register of Trust and Register of Beneficial Ownership. Access to the Register of Trust is public, whilst access to BO Register is provided only to state authorities, obliged entities and parties with legitimate interests. The legal obligation of registered natural persons is to provide information on their BO (name, address, date of the birth, nationality, share of voting and economic rights). The registrar court does not register information about the BO in the Register of Beneficial Owners if the application for registration of information on the BO:

i) was not submitted by a person entitled to apply,

ii) was not submitted by the prescribed procedure,

iii) does not contain all prescribed formalities,

iv) is incomprehensible or vague,

v) was not submitted along with instruments which are supposed to, pursuant to law, demonstrate facts about the beneficial owner.

96. In this case, the registrar court sends a notification to the applicant within the time limit of 3 working days from the receipt of the application and states the reasons for the non-performance of the registration, including instructions on how to redress the deficiencies. However, there seems to be no provision in the law on sanctioning in case of non-provision or provision of false BO information.

97. The Accounting Act stipulates archiving time for accounting documents (records of transactions). The archiving time is 5 years. The Tax Administration is authorised to demand accounting documents within tax control.

98. *Criterion 8.4* –

a) CzR legislation provides for supervision with regard to record-keeping requirements. The supervision is conducted by the Registry Court and Ministry of Culture. All legal persons registered in a public register (within the meaning of the PRA) are obliged to communicate to the Registry Court facts and submit documents necessary for a decision in a procedure initiated without a proposal and submit documents to be deposited according to the law to the collection of documents. The same obligations also apply to religious organizations applying for registration. Additionally, the Tax Administration is authorised to demand accounting documents from accounting units within tax control. As for supervision with regard to BO information, according to Income Tax Act, provided voluntary benefits (such as gifts) are proved by the donor by a document from which it must be clear who is the beneficiary of the voluntary benefit, the value of the voluntary benefit, the subject of the voluntary benefit, the purpose for which the voluntary benefit was provided and the date of the provision of the voluntary benefit. No further information is provided on how the accuracy of the provided BO information is checked. In addition, there seems to be no risk-based supervision in place to be applied to NPOs as risk of FT abuse.

b) Section 104 of the PRA Act articulates that, in case of violation of the legal obligations stipulated under the law, the register courts may repeatedly impose a fine up to 100 000 CZK/EUR 3,877. In case of repeated failure to fulfil this obligation, if there is a legal interest therein and if it can have serious consequences for third parties, the Registry Court may, under Section 105 of the PRA, initiate proceedings on the cancellation of the registered person with liquidation. The court should however provide the registered person reasonable period to remedy the deficiencies. As provided in the NRA, however, because of the large number of

persons newly registered in the Registers, it is not principally possible to check in advance whether the electronically transmitted documents are actually those documents to be stored in the public register. At the same time, legal regulation and the technical functioning of public registers are not set up so as to quickly and timely reveal a mere formal fulfilment of obligations by sending blank electronic documents.

99. In case of registered churches and religious legal persons the supervision on compliance with the requirements with the Act on Churches and Religious Societies is conducted by the Ministry of Culture. If the Ministry of Culture finds that a registered church and a religious society or association of churches and religious societies is operating in violation of some of the provisions of Act it commences the procedure for the cancellation of registration (unless the prior notice of abandonment of this activity has been respected), as well as in cases where a statutory body of a registered church or religious society, or a statutory body of the Union of Churches and Religious Societies is not established for more than two years. In the case of registered legal persons, the Ministry of Culture will cancel their registry if they violate relevant provisions of the Act on Churches and Religious Societies and the competent authority of the Church and the religious society, even after the Ministry's request has not remedied shortcomings, or there is no statutory body of a registered legal person for more than one year.

100. *Criterion 8.5* –

a) Most information is available online, and information concerning NPOs can be accessed administratively or in the course of a criminal investigation. BO information held with the Register on Beneficial Ownership will be available for state authorities and LEAs starting from January 2020.

b) Investigational capacities of the Czech Police are concentrated within the National Organised Crime Agency (NOCA). Within the NOCA operates the Counter Terrorism and Extremism Command, with a specialised central communications, information and analytical department of the Police. These departments are engaged in collecting, evaluating, analysing and processing information found by the Czech Police on terrorists and persons reasonably suspected of being connected to terrorist organizations. According to the NRA, the Command is linked to all departments of the Czech Police and cooperates with other authorities concerned, including the FAU and including foreign competent authorities.

c) As provided under criterion 8.5.a most of the information on NPOs is kept in public registries which are free to access. BO information is also accessible for LEAs. Additionally, there seems to be no restriction on access to information kept by the NPOs.

d) No specific mechanisms for reporting suspected FT-related activity in the NPO sector exists. However, according to Section 18 of the AML Act, the obliged entities are obliged to file an STR to the FAU in case of suspicion of FT, which in its turn should lodge a report to the LEAs (Section 20 of the AML Act).

101. *Criterion 8.6* – Within National Unit against Organised Crime there is national contact point for Terrorism (NCPT), one of the aims of which is to ensure the cooperation with international partners. MLA requests thus would be sent to NCPT. Besides, FAU carries out international cooperation with its counterparts, to which requests can be sent from foreign FIUs.

Weighting and conclusion

102. CzR authorities have conducted a formal review of the NPO sector aimed at identifying possible vulnerabilities for FT abuse. In the course of this exercise adequacy of legislation has been

reviewed as well. However, the country still lacks outreach on FT issues, targeted risk-based supervision/monitoring of NPOs and effective co-operation, co-ordination and information-sharing with the private sector. **Czech Republic is PC with R.8.**

Recommendation 9 – Financial institution secrecy laws

103. The Czech Republic was rated Compliant for R.4 in its 4th round MER.

104. *Criterion 9.1* – S.38 of the AML/CFT Act stipulates that the obliged entities shall maintain confidential facts relating to suspicious transaction reports and their investigation. S.39 AML/CFT Act provides for the exemptions from this requirement to maintain confidentiality. The exemptions apply to competent domestic authorities and relevant foreign authorities. S.39 permits to share information with the competent authorities, including foreign AML/CFT competent authorities and international organisations. S.39(2) stipulates that the obligation of confidentiality shall not be invoked when information is shared between credit and financial institutions, as well as auditors, tax advisors, chartered accountants and court bailiffs.

105. The sectorial acts also provide for an exemption with respect to AML/CFT from the requirement to keep information confidential, namely: S.25a(4)(f) Act on Banks, S.25b(2) Act on Credit Unions, S.117 Capital Market Undertakings, S.640 Act on Investment Companies and Investment Funds, S.128(6) and (7) Insurance Act, S.135b Act on Payment Services (old), S.17(4) Act on Bureau-de-change Activity, S.137 Act on Consumer Credit.

Weighting and Conclusion

106. **Czech Republic is C with R.9**.

Recommendation 10 – Customer due diligence

107. The Czech Republic was rated as Partially Compliant for R.5 in its 4th round MER. Deficiencies were identified with respect to, among others, identification and verification of the beneficial ownership.

108. *Criterion 10.1* – Even though there is no explicit restriction to maintain anonymous accounts, or accounts with fictitious names, the obliged entities are not permitted to keep anonymous accounts, or accounts with fictitious names due to the identification and verification requirements set out in the AML/CFT Act. In addition, the REs are prohibited from opening business relationships or carrying out transactions without CDD being completed as described under s. 15 of the AML/CFT Act (please also see EC.10.19).

109. *Criterion 10.2* –

a) In accordance with S.7(2)(b) and S.9(1)(a) AML/CFT Act, the obliged entities shall perform CDD prior to establishing a business relationship.

b) In accordance with S.7(1) AML/CFT Act obliged entities have to identify the customer when it is obvious that the transaction amount exceeds EUR 1,000. According to S.9(1)(a)(1) CDD shall be carried out prior to a transaction when the value is EUR 15,000 or more. S.54(4) stipulates that if a payment is divided into several instalments, the value of the transaction shall be the sum of these instalments, provided they are related.

c) S.7(1) AML/CFT Act requires obliged entities to identify the customer when it is obvious that the transaction amount exceeds EUR 1,000. With regards to wire transfers, EU Regulation 2015/847 directly applies to the Czech Republic.

d) S.9(1)(b) and S. 7(2)(a) AML/CFT Act stipulate the obligation to perform CDD when there is a suspicious transaction, regardless the value of 1,000 EURO stipulated above.

e) There is no explicit requirement to undertake CDD when there are doubts about the veracity or adequacy of the identification data, however, this is implied through a combination of requirements. S.8(7) and S.15(1)c AML/CFT Act require obliged entities to ensure on an on-going basis that customer data is kept up-to-date and to not establish or to end an existing business relationship, if there are doubts about the veracity or authenticity of CDD information. Based on these two provisions, together with S.6(1)i), obliged entities have to ensure that the information they hold is correct and up-to-date and should they not be able to comply with this obligation, end the relationship and file an STR.

110. *Criterion 10.3* – S.7(2) of the AML/CFT Act requires the obliged entity to always identify the customer. S.8(1)(a) AML/CFT Act stipulates precisely how the obliged entities are to identify natural persons and legal persons. The identification is performed in the personal presence of the customer or the person acting on behalf of a legal person. S.8(2)(a) and (b) stipulate that identities of natural and legal persons are verified through a certificate of identity or through an official record establishing the legal person. There is no reference to legal arrangements and because there is no definition of 'customer' it is not obvious that legal arrangements are included. Nonetheless S9(2)(b) makes clear that the word "customer" incudes both legal persons and legal arrangements.

111. The identification data for natural person, legal persons and trusts or other legal arrangements are defined in the S.5(1)(a-c). S.4(6) defines a "certificate of identity" to mean the card issued by a public administration authority bearing the holder's name and surname, date of birth together with image and potentially other identification features enabling identification of the bearer as the true holder. Although for natural persons this can be seen as a reliable, independent source document, there is no equivalent requirement that the verification of the identity of legal persons and legal arrangements should be based on reliable, independent sources and information.

112. *Criterion 10.4* – In accordance with S.8(1) and (4) AML/CFT Act, the obliged entity shall identify any natural person acting on behalf of a legal person in his/her personal presence. In case the customer is represented based on a power of attorney, the obliged entity shall perform identification and verification of the plenipotentiary (meaning the authorised representative of a person empowered to act) through a certificate of identity and obtain the power of attorney. This is similar when the customer is represented by a statutory agent or a guardian (S.8(5)). When representing a customer, the statutory agent or guardian has to submit identification data of the customer, and the guardian must submit the relevant court decision. S.54(9) AML/CFT Act stipulates that the requirements of the AML/CFT Act concerning the customer shall also apply to a person acting on behalf of a customer – hence should the customer be represented by a legal person, identification to the same extent should be made as if the legal person was the customer. There is no explicit requirement that any person acting on behalf of a legal arrangement is so authorised.

113. *Criterion 10.5* – S.9(2)(b) AML/CFT Act stipulates the obligation to identify the beneficial owner and the adoption of measures to verify the identity of the beneficial owner. A beneficial owner is defined in S.4(4) AML/CFT Act as a natural person having factual or legal possibility to realize directly or indirectly decisive influence in legal person, trust or other legal arrangement without legal personality. Although this is not fully consistent with FATF definition as it does not include natural persons on whose behalf a transaction is being carried out the AML/CFT Act covers the situations where the REs have doubts that the client is not acting on his behalf S8(8).

114. The FAU issued Methodological Instruction No 3 aimed to assist obliged entities in identifying and verifying the identity of the beneficial owner. It includes some guidance on the

verification through information from independent sources, but the instruction is not mandatory. There is therefore no requirement using the relevant information or data obtained from a reliable source to verify the identity of the beneficial owner.

115. *Criterion 10.6* – S.9(2)(a) AML/CFT Act specifies the requirement that the obliged entities collect information on the purpose and intended nature of the transaction or a business relationship. There is no obligation to also understand the purpose and intended nature of the business relationship.

116. *Criterion 10.7* – a) S.9(1)(c) AML/CFT Act requires obliged entities to undertake CDD during the duration of the business relationship. S.9(2)(c) and (d) comply with the FATF requirement of scrutinizing transactions performed throughout the course of the business relationship, to identify if the transactions are consistent with the obliged entity's knowledge of the customer, business and risk profile, including source of funds. b) S.8(7) AML/CFT Act requires that the obliged entities control the validity and completeness of the customer's identification data (as defined in S.5 as data on names, identification number, place of birth, place of business, etc.). There is no specific provision for higher risk categories of customers. The evaluation team is satisfied that the requirement to keep the information "valid and complete" covers the need to keep the information relevant and up-to-date.

117. *Criterion 10.8* – S.9(2)(b) AML/CFT Act requires obliged entities, in case the customer is a legal person, a trust or other legal arrangement without legal personality, to establish the ownership and control structure of the customer. The AT is confident that the word "establish" covers the concept of "understand" as required by the standard. It is not specifically required to understand the nature of the customer's business beyond the requirements of S.9(2)(a) and (c) AML/CFT Act as described under EC10.6 and EC10.7.

118. *Criterion 10.9* – The identification data for legal entities and legal arrangements are set out in the S.5(1)(b) and (c) AML/CFT Act, and includes:

- For legal persons – name of the business, including appendices and other features; its registered office and business identification number; as well as verify them through a document on existence. Natural persons, acting on behalf of these legal persons are also identified.
- For trusts and legal arrangements without legal personality – name of the business, including appendices and other features; its registered office and identification number; for the trustees, administrators and persons in similar positions - name, date of birth, sex, residence and citizenship.

119. Verification of the identity of legal persons and proof of existence is set out in S.8(2)(b) AML/CFT Act. There is a requirement to identify the registered office of legal entities and legal arrangements. For legal persons and legal arrangements, information on the name, legal form, statutory body and its members, controlling body and its members, address of the office, or of principal place of business, if these two differ, can be verified in the S.25(1) Act on the Public Registries of the Legal and Natural Persons. The registry is a publicly available database. The AML/CFT Act does not specify the requirement to identify proof of existence of legal arrangements.

120. *Criterion 10.10* –

a) S.9(2)(b) of the AML/CFT Act stipulates that the beneficial owner of a legal entity is identified, and measures are adopted enabling the obliged entity to identify and verify the identity of the beneficial owner. S.4(4) stipulates the controlling ownership percentage as 25%.

b) b) S. 4(4)(a)(2) includes as a beneficial owner the person who alone or in connection with other persons acting in concert with the natural person controls the legal entity. The definition does include "a natural person having factual or legal possibility to realize directly or indirectly decisive influence in legal person, trust or other legal arrangement without legal personality". This covers the control over the legal person or arrangement through "other" means as provided by the Methodology.

c) c) S.4(4)(a)(4) states that is if there is no beneficial owner or it is not possible to determine a beneficial owner a member of a statutory body, representative of legal person in such body and/or in position similar to member of statutory body will be considered as the beneficial owner. Although there is no specific requirement to identify the "senior management", the assessment team's understanding is that this is covered by the expression "a member of a statutory body".

121. *Criterion 10.11* – S.4(4) AML/CFT Act considers as the beneficial owner of a trust or other legal arrangement without legal personality a natural person or beneficial owner of a legal person, who is in a position of a founder, a trustee, a beneficiary, a person in whose interests the trust or other legal arrangement was established or is functioning if a beneficiary is not determined, and persons allowed to maintain supervision on administration of the trust or other legal arrangement without legal personality (which according to S.4.4(c)(5) includes the protector and other natural persons exercising ultimate effective control). S.9(6)(b) requires that the obliged entity collects and records for a beneficiary of a trust or other legal arrangement who is determined based on particular characteristics or membership of particular category, the information necessary to identify the particular beneficiary in the moment of payment of returns or in the moment of exercise of beneficiary's rights.

122. S.9(2)(b) AML/CFT Act requires the adoption of measures in identifying and verifying the identity of the beneficial owners of trusts or other legal arrangements. For trusts and other legal arrangements, the names and identification data of trustees, administrators or a person in similar positions need to be obtained (S.5(1)(c)).

123. *Criterion 10.12* - a) S.9(6)(c) requires that the obliged entity collects and records for the beneficiary who is determined as a particular person or a legal arrangement without legal personality, data about the name and surname or name of the legal person. b) For a beneficiary who is determined based on the characteristics of the relationship with the person insured or otherwise, the data necessary to identify the particular authorised person in the moment of a payment has to be collected and recorded. c) Persons entitled to receive a life insurance settlement (beneficiary) are to be identified at the latest on the day of payment (S.7(3) AML/CFT Act).

124. *Criterion 10.13* – There are no specific requirements for the obliged entities to include the beneficiary of a life insurance policy as a relevant risk factor when determining whether to apply enhanced CDD measures. S.5(3)c CNB Decree requires financial institutions to undertake enhanced monitoring with regard to transactions (such as the pay-out of an insurance policy) which contain a risk factor set out in S.5(2) of the CNB Decree (such as an unusual manner of undertaking the transaction).

125. *Criterion 10.14* – Identification and verification of identity of the customer and the beneficial owner is required prior to conducting a transaction out of business relationship (occasional transaction), if the transaction exceeds the EUR 15,000 threshold (S.9(1)(a)), or prior to establishment of any business relationship (S.9(1)(b)). It is not permitted to complete verification after the establishment of the business relationship.

126. *Criterion 10.15* – The AML/CFT Act does not permit utilization of business relationships prior to verification of the customer's identity.

127. *Criterion 10.16* – During the business relationship or when performing other transactions obliged entities have to control the validity and completeness of customer's identification data (S.8(7)). Also, CDD has to be undertaken during the duration of the business relationship (S.9(1)(c)). The AML/CFT Act does not specifically require CDD for existing customers when new requirements are brought into force, however, new CDD requirements are always applied to all obliged entity's customers. There is no requirement to do this on the basis of materiality and risk nor to take into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

128. *Criterion 10.17* – The AML/CFT Act does not explicitly require obliged entities to perform EDD where the ML/FT risks are higher. Nonetheless the obliged entities have to perform on-going monitoring and scrutiny of the sources of funds to the extent necessary by taking into account the risk factors stipulated in the risk assessment and the ML/FT risks of the type of customer, business relationship, product or transaction (S9(2) (c) and (d), S9(3)). Furthermore, S.5(1) of the CNB Decree on certain requirements for the system of internal principles, procedures and control measures against ML/FT (which is a legally binding document) provides that financial institutions should apply risk management measures commensurate with the risk profile of the customer. It lists risk indicators (such as geographical risks, business profiles, ownership structure etc.) and stipulates an obligation to undertake enhanced scrutiny in case of transaction where a high risk factor is present.

129. *Criterion 10.18* – S.13(1) AML/CFT Act lists categories of customers with potential lower risk levels where the obliged entities may apply simplified CDD (SDD). However, these lower risk customer categories have not been identified through an adequate analysis of risks by the country or the financial institution. S.13(4) prohibits application of SDD to PEPs. S.13(3) (c) limits the application of SDD should any of the customers, provided products or particular transaction present a higher risk of abuse for legitimisation of proceeds of crime or financing of terrorism . Other higher risk scenarios are not explicitly listed.

130. *Criterion 10.19* – a) When the obliged entity is unable to comply with relevant CDD measures, it should refuse to perform a transaction, establish business relationship (which includes opening an account) or terminate existing business relationship (S.15(1)). b) If a customer refuses to undergo CDD, or refuses to submit the identification data, the obliged entity shall submit an STR (S.6(2)(c) AML/CFT Act). This STR reporting does not broadly extent to the circumstance when a financial institution is unable to comply with the relevant CDD measures.

131. *Criterion 10.20* – There is no explicit provision in the AML/CFT Act enabling the obliged entities not to apply CDD if there is a risk of tipping-off the customer, and in that case, report a STR.

Weighting and conclusion

132. Czech Republic meets the requirements of C. 10.2, 10.10, 10.11, 10.12, 10.14, 10.15; mostly meets 10.1, 10.3, 10.4, 10.6, 10.7, 10.8, 10.9, 10.19; partly meets 10.5, 10.13, 10.16, 10.17, 10.18 and does not met 10.20. The main deficiencies relate to insufficient requirements for: deficiencies in definition of beneficial owner; CDD in case of legal arrangements; application of EDD where the ML/FT risks are higher; determining the relevant risk factors for enhanced CDD measures for life insurance policies; and determining risk scenarios in all cases. There is no explicit provision in case of risk of tipping-off the customer followed by submission of a STR. **The Czech Republic is LC with R.10**.

Recommendation 11 – Record-keeping

133. The Czech Republic was rated Largely Compliant in its 4th round MER for R.10. There was no provision to maintain records for a longer period when it was required by the FAU in special circumstances, there was no explicit requirement to maintain records in a way suitable to reconstruct individual transactions and there was no specific requirement to retain business correspondence for at least five years following the termination of an account or a business relationship.

134. *Criterion 11.1* – Obliged entities have to store data and documents on transactions related to the obligation of identification for at least 10 years following the transaction or the termination of the business relationship (S.16(2) AML/CFT Act). The requirement concerns both domestic and international cases, but no distinction is made explicitly between these two.

135. *Criterion 11.2* – S.16(1) AML/CFT Act stipulates that the obliged entities keep for 10 years after the transaction or termination of business relationship the identification data and other documents obtained during CDD. There is no clear requirement in the AML/CFT law to maintain records on account files, business correspondence and/or results of any relevant analysis, however, S.7 CNB Decree requires financial institutions to have an information storage system, which has to include information about findings made when inspecting a customer and examining transactions and correspondence relating to transactions and business relationships.

136. *Criterion 11.3* – There is no requirement to maintain transaction records in a manner enabling reconstruction of individual transactions to assist investigations.

137. *Criterion 11.4* – S.24 AML/CFT Act grants permission to the FAU for access to the transaction related to the identification obligation. Article 39 provides for an exemption from confidentiality for law enforcement and supervisory authorities. See R.27 and R.28 for access by supervisors to CDD and other data.

Weighting and conclusion

138. Most of the requirements in terms of record keeping are satisfied, but obliged entities are not required to retain the records in a way suitable to reconstruct individual transactions**. The Czech Republic is LC with R.11.**

Recommendation 12 – Politically exposed persons

139. The Czech Republic was rated Partially Compliant in its 4th round MER. Certain types of PEPs were not defined; there was no requirement to consider if a beneficial owner was a PEP; approval was not specified to be at the level of senior management.

140. *Criterion 12.1* - S.4(5) of the AML/CFT Act defines PEPs. The AML/CFT Act does not distinguish between domestic and foreign PEPs. This definition is consistent with the FATF definition, although the wording does not specifically include “senior politicians” and “important political party officials.” However, those functions are covered by the inclusion of “members of governing bodies of political parties” (which are in fact “senior/important politicians”). The definition also includes a beneficial owner of a legal person, a trust or any other legal arrangement without legal personality and a beneficial owner of a legal person, a trust or other legal arrangement without legal personality known to the obliged entity as a person created in favour of a PEP. The definition of PEP includes a natural person, who is or was in similar function in other state or in European Union body and/or in international organisation.

a) In accordance with S.8(3) an obliged entity has to check within the identification process whether the customer is a PEP. S.21(5) requires obliged entities to have a system of internal rules that covers measures how to detect PEPs. The internal rules should be based on the risk assessment stipulated in S.21a.

b) S.15(3)(a) requires approval of the statutory body of the obliged entity or person authorised by the statutory body in management for a business relationship with a PEP. This would equal senior management and also implies both establishment and continuation (for existing customers) of the business relationship.

c) CDD for any customer involves scrutiny of the sources of funds or other property affected by a transaction or business relationship (S.9(2)(d)). S.9(2)(e) additionally states that within a business relationship with a PEP also adequate measures for identification of the origin of his/her funds should be taken. The obliged entity is not permitted to realize a transaction with a PEP, if the origin of the property used in the transaction is not known (S.15(2)). There is no clear reference to source of wealth, but this is encompassed by the source of other property.

d) The AML/CFT Act prohibits SDD for PEPs (S.13). There is no clear requirement to conduct enhanced on-going monitoring on the relationship with a PEP, however, S.9(2)(c) requires on-going monitoring consistent with the customer's risk profile and S.5(3)(c) CNB Decree requires financial institutions to pay special attention to transactions by PEP.

The obliged entity has to apply these same measures towards a client whose beneficial owner is a PEP and towards a person which is known to be acting on behalf of a PEP (S.54(8) AML/CFT Act). This section also stipulates that obligations and limitations related to PEPs shall be applied by obliged entities within 12 months since the day that PEP terminates to perform a relevant position at least, but always until obliged entity will eliminate on the basis of the risk assessment risk specific for the PEP. This is in line with FATF guidance that points towards a more RBA and (specifically) not on prescribed time limits.

141. *Criterion 12.2* – a) As aforementioned, c.12.1 (a) analysis applies to 12.2 (a); b) the Czech law does not specifically provide for measures when there is a high risk business relationship with a domestic PEPs, but as aforementioned, c.12.1 b)-d) also apply to c.12.

142. *Criterion 12.3* – The definition of PEP includes a natural person, who is a person known to be a close associate of a PEP, a business partner of a PEP or a natural person who is known to the obliged entity as a person in a close business relationship with a PEP. In S.22(1) Civil Code is a close associate defined as a relative in direct line, sibling and spouse or partner, or other person in similar relationship.

143. *Criterion 12.4* – S.9(6)(c) AML/CFT Act requires that the obliged entity collects and records information on all relevant circumstances and the process of the business relationship with respect to a person who is the beneficiary of life insurances and who is a PEP. This requirement does not extend to the beneficial owner of the beneficiary. With respect to the timing the general provision of S.7(3) applies stating that person entitled to receive the life insurance settlement shall be identified at the latest on the day of the payment. There is no requirement to inform senior management when higher risks are identified, to conduct enhanced scrutiny on the whole business relationship.

Weighting and conclusion

144. Certain deficiencies, although considered minor, are noted with respect to beneficiaries of life insurances that are PEPs. **The Czech Republic is LC with R.12**.

Recommendation 13 – Correspondent banking

145. The Czech Republic was rated as Largely Compliant for R.7 in the previous round. More banking regulations were needed to better address various requirements. The scope of the requirements also had to be broad beyond banks.

146. *Criterion 13.1* – The definition of correspondent banking (S.4(7) AML/CFT Act) refers to banks, as well as the relationships between credit institutions, financial institutions and credit and financial institutions where similar services are provided, and including relationships established for securities transactions or funds transfers.

a) S.25(2) and 25(3) AML/CFT Act require that prior to the establishment of a correspondent relationship with a respondent institution, the credit or financial institution gathers sufficient information about the respondent institution and the nature of its business and other risk factors, and detects based on publicly available information on the quality of supervision imposed on the respondent institution. This does implicitly include information on whether the respondent institution has been subject to AML/CTF investigation or regulatory action.

b) The credit or financial institution shall also detect and assess the quality of the respondent institution's AML/CFT measures and quality of CDD performed and its ability to provide this information upon request as well as the ability to provide information about payer in case of funds transfers.

c) The statutory body of the credit or financial institution or the branch manager of the foreign credit or financial institution operating in the territory of the Czech Republic has to agree with the establishment of the correspondent relationship. This would satisfy C.13.1.c.

d) There is no requirement to understand the AML/CFT responsibilities of the institutions engaged in the correspondent banking.

147. *Criterion 13.2* – There is no explicit requirement in the AML/CFT Act regarding payable-through-accounts. Based on the general requirements for correspondent banking (S.25(2)(c)) the credit or financial institution should assess the ability of the respondent institution to provide CDD information upon request which would cover EC 13.2 (b).

148. *Criterion 13.3* – S.25(1) AML/CFT Act does not permit the obliged entity to enter into a correspondent relationship with institutions "registered in the business or similar register in a country, where it is not factually presented not even its real management and which is not affiliated to any regulated financial group". This definition is consistent with the FATF Glossary definition of shell banks.

Weighting and Conclusion

The law does not regulate payable-through-accounts, nor to understand the AML/CFT responsibilities of the institutions engaged in the correspondent banking. **The Czech Republic is PC with R.13**.

Recommendation 14 – Money or value transfer services

149. The Czech Republic was rated as Partially Compliant in it 4th round MER. Effective implementation of SR.VI was not demonstrated, and alleged informal remittance activities were not fully assessed. On 13 January 2018 a new Act on Payment Services (Act no. 370/2017) entered into force. This new act transposes the requirements of the EU Payment Services Directive II.

150. *Criterion 14.1* – MVTS are obliged entities under the S.2(1)(b)(11) AML/CFT Act and Act on Payment Services lists the institutions permitted to provide payment services. These institutions have to be authorised by the CNB, pursuant to the S.7 and S.66 of the new Act on Payment Services, and are subject to the CNB supervision. S.66 concerns electronic money institutions which are also allowed to provide money transfers.

151. *Criterion 14.2* – The CNB has indicated that it uses a variety of supervisory mechanisms to identify MVTS providers without a license (e.g. offsite supervision activities, monitoring online activities of MVTS providers or investigation of external information/notice on business activity without appropriate license, especially in co-operation with the police). The Act on Payment Services and the Act on Bureau-de-change Activity authorizes the CNB to request information from MVTS to verify if the operation is performed with a license or registration. A fine up to CZK 50,000,000 (almost EUR 2 million) can be given by CNB if the entity fails to provide the required information. The CNB can also cease operation of an unauthorised MVTS. Additionally, any alternative business operation is considered as an unauthorised business activity under S.251 Criminal Code.

152. *Criterion 14.3* – MVTS are obliged entities under the AML/CFT Act, and are therefore subject to monitoring of AML/CFT compliance in concurrence with S.35. In accordance with S.237 of the new Act on Payment Services, the CNB supervises compliance by MVTS. CNB performs both onsite and offsite supervision of MVTS (see R.26, R.27).

153. *Criterion 14.4* – According to S.25 of the new Act on Payment Services, money transfer/payment services may be provided via authorised agents if the service provider notifies this fact to the CNB. The CNB maintains a list of all payment institutions together with the agents through which they provide services (S.26 Act on Payment Services). The CNB has to access the list of agents of MVTS that are licensed in other EEA countries but operating in the Czech Republic through the home supervisor of that MVTS.

154. *Criterion 14.5* – S.19 and 20 of the new Act on Payment Services requires payment institutions/MVTS to have an internal control system which should include on-going monitoring of compliance with legal obligations set out in the Act on Payment Services or any other legal regulation. This system also includes the rules of control of the activities of authorised agents through which the payment institution provides payment services. Payment institutions are required to verify and regularly evaluate the adequacy and the effectiveness of the management and control system.

155. In accordance with S.21(5)(g) AML/CFT Act, the system of internal rules has to cover the procedures and rules to be followed by a third party (such as an agent) when offering products or services on behalf or on the account of the obliged entity. In addition, S.54(6) AML/CFT Act requires an obliged entity under whose name or on whose account products or services are marketed by third parties to ensure that these third parties observe all the procedures against the legitimisation of proceeds of crime and financing of terrorism in the same scope as the obliged entity.

Weighting and Conclusion

156. **The Czech Republic is C with R.14.**

Recommendation 15 – New technologies

157. The Czech Republic was rated as Partially Compliant in its 4th round MER. As mentioned in that report, there were several deficiencies such as no specific requirement requiring financial institutions to have policies in place or to take measures as may be needed to prevent the misuse of technological developments.

158. *Criterion 15.1* – S.21a AML/CFT Act requires obliged entities to assess the ML/FT risks taking into consideration the factors of potential higher risk stipulated in Annex No 2 of the AML/CFT Act, which includes "new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products". In addition, certain obliged entities (inter alia, banks and other financial institutions) have to develop a written assessment of the ML/FT risks upon becoming an obliged entity. This risk assessment should be updated regularly, in particular prior to initiation of new products.

159. The FAU has issued a Methodological Instruction No 2 regarding virtual currencies. It provides a general short overview of the product and approach to it. The CNB participated in the preparation of the EU Opinion on the use of innovative solutions by credit and financial institutions in the CDD process, which was published on 23 January 2018. This Opinion will be published on the website of the CNB. The assessment of risks associated with new products, technologies and practices is included at certain points throughout the NRA. However, in the absence of a dedicated chapter dealing with new technologies and products, it is difficult to assess the completeness of such evaluation for c. 15.1 purposes.

160. *Criterion 15.2* –According to S(21a) (1) and S(30a) (2) the obliged entities have to update regularly their risk assessment, in particular prior to development of new products (S.21a(4) AML/CFT Act). The Annex 2, provides the non-exhaustive list of factors and types of evidence of potentially higher risk and should be taken into consideration when up-dating the risk assessment. Annex 2 includes new products and new business practices, new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products. The entities also have to take appropriate measures to mitigate the risks (S.21(1) AML/CFT Act). There is no specific requirement for the up-date the risk assessment prior to the launch or use of such technologies.

Weighting and Conclusion

161. Both criteria are mostly met, therefore, **the Czech Republic is LC with R.15.**

Recommendation 16 – Wire transfers

162. The Czech Republic was rated as Largely Compliant in its 4th round MER. There were several deficiencies. EU Regulation 2015/847 came into force on 26 June 2017 and is directly applicable to all EU member states. With respect to FATF R.16 domestic wire transfers are wire transfers within the EU; and wire transfers refers to wire transfers outside the EU.

163. *Criterion 16.1* –

a) According to the EU Regulation (S.4) all wire transfers exceeding EUR 1,000 shall be accompanied by the following information on the payer (the originator): the name of the payer; the payer's payment account number; the payer's address, official personal document number, customer identification number or date and place of birth. In case of a transfer not made from or to a payment account, the payment service provider of the payer shall ensure that the transfer of funds is accompanied by a unique transaction identifier. The payment service provider of the payer has the obligation to always verify the accuracy of the above mentioned information on the payer on the basis of documents, data or information obtained from a reliable and independent source before transferring funds.

b) All wire transfers exceeding EUR 1,000 shall be accompanied by the following information on the payee (beneficiary): the name of the payee; the payee's payment account number. In the case of a

transfer not made from or to a payment account, the payment service provider of the payer shall ensure that the transfer of funds is accompanied by a unique transaction identifier.

164. *Criterion 16.2* - In the case of a batch file transfer from a single payer where the payment service provider of the payee is established outside the EU (cross-border transfer), there is no need to provide individual transfer data, provided that the batch file contains the information on payer, payee and unique transaction identifier when transfers are not made from or to an account and that that information has been verified and that the individual transfers carry the payment account number of the payer or unique transaction identifier (S.6(1)).

165. *Criterion 16.3* - If the transfer value does not exceed EUR 1,000 (and when it does not appear to be linked to other transfers of funds which together with the transfer in question exceed EUR 1,000), the wire transfer must be accompanied with the names of the originator and beneficiary, their account numbers, or were applicable – unique transaction reference numbers (S.6(2)).

166. *Criterion 16.4* – S.6(2) Regulation states that the payer's payment service provider need not verify the information on the payer unless the payment service provider of the payer has reasonable grounds for suspecting money laundering or terrorist financing. Additionally, S.9(1)(b) AML/CFT Act requires that suspicious transactions are always subject of CDD.

167. *Criterion 16.5* – S.5(1) Regulation stipulates that all payment service providers involved in the payment chain that are established in the EU (=domestic), ensure that transfers of funds are accompanied by at least the payment account number of both the payer and the payee or, in the case of a transfer not made from or to a payment account, the unique transaction identifier. S.5(2) Regulation states that the payment service provider of the payer shall, within three working days of receiving a request for information from the payment service provider of the payee or from the intermediary payment service provider, make available the required information. As described in R9, the authorities can have access to the information held at the obliged entities.

168. *Criterion 16.6* – S.5(2) Regulation states that the payment service provider of the payer shall, within three working days of receiving a request for information from the payment service provider of the payee or from the intermediary payment service provider, make available the required information. As described in R9, the authorities can have access to the information held at the obliged entities. In case a payment service provider uses a unique transaction identifier, this should be a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, which permits the traceability of the transaction back to the payer and the payee. As described in R.31 law enforcement authorities are able to compel immediate production of information.

169. *Criterion 16.7* – The identification data obtained under the CDD requirements or based on EU Regulation 2015/847 must be retained be the ordering obliged entity for at least 10 years after the transaction (S.16 of the AML/CFT Act) , but the data is not complete as required by the Recommendation 11.

170. *Criterion 16.8* – The ordering obliged entity shall not execute any transfer of funds if it does not comply with above mentioned 16.1-16.7 criteria (S.4(6) Regulation).

171. *Criterion 16.9* – The intermediary payment service providers shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer (S.10 Regulation).

172. *Criterion 16.10* – S.11(1) of the EU Regulation does not make specific exemptions for technical limitation relevant to this criterion. All identification data obtained under the CDD requirements or based on EU Regulation 2015/847 must be retained by the intermediary obliged entity for at least 10 years after the transaction (S.16 AML/CFT Act).

173. *Criterion 16.11* – The intermediary entity shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the information on the payer or the payee is missing for transfers of funds where the payment service provider of the payer or of the payee is established outside the EU. This also applies for batch file transfers where the payment service provider of the payer or of the payee is established outside the EU (S.11(2) Regulation).

174. *Criterion 16.12* – The intermediary entity should have effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow up action (S.12 Regulation). If the service provider has not been provided with the required payer or payee data, it shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the transfer of funds, on a risk-sensitive basis.

175. *Criterion 16.13* – The obliged entity of the beneficiary shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the following information on the payer or the payee is missing for transfers of funds where the payment service provider of the payer is established outside the EU, as well as for batch file transfers where the payment service provider of the payer is established outside the EU (S.7(2) Regulation).

176. *Criterion 16.14* – S.7(3) Regulation requires the beneficiary entity in case of transfers of funds exceeding EUR 1,000, before crediting the payee's payment account or making the funds available to the payee, to verify the accuracy of the information on the payee on the basis of documents, data or information obtained from a reliable and independent source. The obtained information is not complete as it was described in R11. Verification is deemed to have taken place where a payee's identity has been verified in accordance with the AML/CFT Act and the information obtained pursuant to that verification has been stored in accordance with the AML/CFT Act.

177. *Criterion 16.15* – The beneficiary entity shall implement risk-based procedures to determine whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action. Where the obliged entity of the beneficiary becomes aware, when receiving transfers of funds, that the information is missing or incomplete or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system, the payment service provider of the payee shall reject the transfer or ask for the required information on the payer and the payee before or after crediting the payee's payment account or making the funds available to the payee, on a risk-sensitive basis (S.8 Regulation).

178. *Criterion 16.16* – MVTS as obliged entities are subject to the EU Regulation, as described in R.14. MVTS have to ensure that agents also observe the AML/CFT obligations.

179. *Criterion 16.17* – MVTS are obliged entities under the AML/CFT Act which provides for obligations for the obliged entities to identify and submit STRs. Although there is no specific requirement for a MVTS that controls both the ordering and the beneficiary side of a wire transfer to take into account all the information from both the ordering and beneficiary sides in order to

determine whether an STR has to be filed, MVTS are required to monitor the whole transaction and business relationship.

180. *Criterion 16.18* – Financial institutions have obligation to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373, and their successor resolutions in relation to all transactions which they are taking part in, including wire transfers.

Weighting and Conclusion

181. All essential criteria of R.16 are either met or mostly met. Nonetheless, data on originator and beneficiary information is not fully compliant with R11. **Czech Republic is LC with R.16.**

Recommendation 17 – Reliance on third parties

182. In the 4th Round MER, the Czech Republic was assessed as "not applicable" for R.9 on third party reliance.

183. *Criterion 17.1* – Obliged entities do not have to carry out CDD (including identification of the customer, identification of the beneficial owner, and the nature/purpose of transaction or a business relationship), if it has been performed by another obliged entity under the AML/CFT Act. In this case, the obliged entity is held equally responsible for this activity, as if it has performed the activity itself (S.11(4) AML/CFT Act).

a) In accordance with S.11(3) the obliged entity should ensure that the entity that has performed CDD provides copies of relevant documents on customer's identification, purpose and intended nature of the business relationship, ownership and controlling structure of the customer and identity of the beneficial owner. The identification of the customer under S.8(1) can also be performed by a notary (also a foreign notary if the issued public document can be recognized in the Czech Republic) or the public administration (7000 Czech POINT locations and at 40 embassies abroad) based on a request of the customer or the obliged entity. This identification is in the form of a public document in which it must be stated who, on whose request and for what purpose the identification is performed, and from which document the identity was verified.

b) The law does not specify that the information should be obtained immediately, nor that copies and documentation are to be made available by the third party upon request and without delay.

c) S.11(1) of the AML/CFT Act specifies the domestic and foreign obliged entities that could be relied upon as third parties. Entities licensed in the Czech Republic are also obliged entitles as per S.2 AML/CFT Act, and are therefore subject to regulation and supervision, and have measures to comply with the AML/CFT Act. In case of foreign third parties, these should be from a country that applies similar obligations of customer identification, CDD and record keeping and require obligatory professional licenses and should be a subject to supervision including control of these conditions, the possibility to control each transaction and onsite supervision.

184. *Criterion 17.2* – Obliged entities are not allowed to rely on information from third parties from high-risk third countries with the exception of branches and subsidiaries in an EU member state meeting requirements equal to the EU AML/CFT Law (S.11(10) AML/CFT Act). Regarding the determination of such equivalence the FAU has published on its website a list of countries which meet the criteria of equivalence of their law in the area of combating ML/FT. At the same time, it should be noted, that legislation does not require analysis of ML/FT risks.

185. *Criterion 17.3* – In case a financial institution relies on a third party that is part of the same group, the same requirements as for financial institutions that are not part of a group apply. The description in 17.1 and 17.2 therefore equally applies to financial institutions in a group. S.21a(5) AML/CFT Act requires obliged entities that are part of a group to apply group AML/CFT policies and procedures as allowed by the law of the third country, and policies and procedures for information sharing within the group. These policies and procedures shall also be applied in branches and subsidiaries in EU member states and third countries.

Weighting and Conclusion

186. Although some deficiencies concerning the specific requirement that the information should be obtained immediately and lack of legislative requirement on analysis of ML/FT risks on third party's country of origin, they are consider minor in the context of the country. **Czech Republic is LC with R.17.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

187. The Czech Republic was rated as PC with regards to Internal Controls, Compliance and Audit (R.15), and LC with regards to Foreign Branches and Subsidiaries (R.22) in its 4th round MER.

188. *Criterion 18.1* – S.21 AML/CFT Act requires the obliged entity to introduce and apply AML/CFT internal control policies and procedures to mitigate and effectively manage the ML/FT risks as identified in its risk assessment. a) S.22 requires the designation of a contact employee for fulfilment of the reporting obligation and also for ensuring continuous contact with the FAU if these activities are not directly done by the statutory body. In case the contact person is not someone from the statutory body, the obliged entity has to make sure that the contact person has the possibility of direct communication with the statutory body and supervisory body of the obliged entity. It is unclear if this would imply that the compliance officer is at management level, as there is no such requirement.

b) - d) S.21a(3) AML/CFT Act stipulates that as part of the risk assessment the obliged entity needs to have measures for internal control, control of compliance with laws and security screening of obliged entity's employees and in accordance with the extent and nature of obliged entity's activities also the establishment of an independent unit for testing of the measures, policies and procedures. There is no specific provision requiring screening of employees before hiring, to ensure high standards. c) The requirement for an on-going employee training program is included in S.23 AML/CFT Act.

189. *Criterion 18.2* – a) In accordance with S.21a(5) and 24a obliged entities that are part of a group have to apply group AML/CFT policies and procedures and policies and procedures for information sharing within the group. These policies and procedures have to be applied in branches and subsidiaries in EU member states and third countries. b) There is no requirement in the law regarding the provision at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries, when necessary. c) S.38 requires obliged entities and their employees to keep confidential facts relating to suspicious transaction reports and their investigation. S.39 provides for possibilities to share AML/CFT-related information within a financial group.

190. *Criterion 18.3* – S.24a AML/CFT Act requires that the CDD and record-keeping measures apply to branches and subsidiaries operating outside the EEA at least at the level of the EU law but the requirement does not extend to all AML/CFT measures. If that is not possible, the obliged entity should notify the FAU and apply reasonable additional measures for effective AML/CFT risk

management. Also for branches or business premises within the EU the obliged entity has to ensure that such branch or business premises follow the domestic AML/CFT regulation.

Weighting and Conclusion

191. There are some deficiencies with respect to provision of information at group level compliance and audit functions. Employee screening procedures (before hiring) are not provided for by the law. Also, there is no clear requirement to appoint a compliance officer at management level. **Czech Republic is LC with the R.18.**

Recommendation 19 – Higher-risk countries

192. The Czech Republic was rated Partially Compliant in its 4th round MER. The indirect provisions of the law had to be more specific regarding high-risk countries.

193. *Criterion 19.1* – S.9(1)(a)(3) of the AML/CFT Act requires obliged entities to perform CDD prior to a transaction or a business relationship with a person settled in a country considered as high-risk based on a designation from the EC or for other reason, and regardless of any value threshold. The EC publishes a list of countries that follows the countries listed by the FATF. The FATF list is also published on the FAU website and is publicly available. The S.5 CNB Decree on certain requirements for the system of internal principles, procedures and control measures against ML/FT requires financial institutions to draw up a risk profile of their customers having regard to the fact when the customer is from a higher risk country. In this case the institution should pay special attention to the transactions, but there is no specific obligation to apply EDD.

194. *Criterion 19.2* – The S.25(1) (c) of the AML/CFT Law prohibits FIs to enter into correspondent relationships with banks from countries which do not apply at least similar AML/CFT measures as EU countries. Additionally, Annex 2 of the AML/CFT Law lists as potentially high risk elements countries identified as not having effective AML/CFT systems. The element must be taken into account when assessing the particular risk the obliged entities faces and apply respective mitigating measures.

195. *Criterion 19.3* – Obliged entities received the NRA in which information on other possible risky countries was published. In addition, the FAU provides information from open sources, such as the FATF list of high risk jurisdictions and list of non-cooperating jurisdictions, the EC Delegated Acts on high risk countries, countries with high levels of corruption, drug-related crimes, tax havens, or countries subject to international sanctions.

Weighting and Conclusion

196. *Even* though obliged entities have to take into account information on high risk countries, there is no requirement to apply EDD. Also, the requirement to apply countermeasures is not clear and explicit. **Czech Republic is PC with R.19.**

Recommendation 20 – Reporting of suspicious transaction

197. Czech Republic was rated largely compliant during the 4th round with the former Recommendation 13 and SR. IV. The main reasons for such rating were the concerns related to the efficiency of the reporting requirement being negatively affected by the listing of (suspicious reporting) transactions prescribed by the AML/CFT ACT. In relation to the FT reporting regime, it was noted by the assessors that only "property" linked with a transaction was covered by the reporting obligation.

198. *Criterion 20.1* – The STR reporting obligations are stipulated under Sections 18- 20 of the AML/CFT Act. Suspicious transaction is defined under Section 6 of AML/CFT Act as a transaction the circumstances of which lead to:

i. a suspicion of *legitimisation of proceeds of crime* or

ii. suspicion that funds used for the transaction are determined to be *used for financing of terrorism*, the transaction can otherwise be connected to FT; or

iii. other facts that indicate such suspicion.

199. However, this definition does not seem to cover criminal activities that would constitute a predicate offence for ML, as the legitimization of proceeds of crime, is the corpus delicti of ML offence according to Section 216 of the CC.

200. The same section provides a list of characteristics that could indicate ML/FT suspicion. Part of these characteristics relates to banking operations, while the other part may concern all obliged entities.

201. Section 18 of the AML/CFT Act provides that when the obliged entity detects a suspicious transaction, it should be reported to the FAU without undue delay, no later than 5 calendar days from the day of such detection. Section 26(4) of the AML/CFT Act specifies that certain DNFBPs shall submit a STR to the FAU through the respective Chambers. The latter should refer the STR to the FAU without undue delay, *but no later than 7 calendar days* from the detection of the suspicious transaction. This timeframe seems not to be in line with the notion of "promptness" when compared to the other FATF MERs82. In danger of delay the transaction should be reported immediately after being detected. This provision seems to be rather subjective, for which its application is unclear.

202. Although a major progress is acknowledged with regard to steps taken by the Czech Republic to ensure compliance with the definition of the ML and FT, some minor shortcomings remain (please see the analysis of R. 3 and R. 5) which might have some influence on the scope of reporting under Recommendation 20.

203. *Criterion 20.2* – S.4 of the AML/CFT Act provides the definition of a transaction as any interaction of the obliged entity with another person should such interaction lead to attempted handling of the other person's property or providing services to such other person. Section 6 stipulates that a transaction shall be perceived suspicious if the customer refuses to undergo due diligence process or refuses to submit identification data. The Czech authorities have indicated that according to Sections 4, 6 and 18 of the AML/CFT Law all suspicious transactions, including attempted transactions, are to be reported.

204. No reporting threshold is specified in the law or in the indicators provided by the authorities.

Weighting and Conclusion

205. The definition of STR does not cover criminal activities that would constitute a predicate offence for ML. The reporting timeframe is not in line with the notion of "promptness". **Czech Republic is PC with R.20.**

[82] MERs of Denmark, Ireland, Ukraine, Portugal, Sweden, Switzerland

Recommendation 21 – Tipping-off and confidentiality

206. Czech Republic was not assessed in the 4th round against the requirements of former Recommendation 14 but was rated Largely compliant on this recommendation in the 3rd round given that the protection did not extend explicitly to the disclosure of information (although it covered the suspension of transactions), beyond the obliged entity, to its management and staff.

207. *Criterion 21.1* – Section 18 (3) of the AML/CFT Act states that data on the employee of the obliged entity or on the person in equal position who detected the suspicious transaction should not be mentioned in the report. According to Part 2 of Article 5 of the Personal Data Protection Act, in case the data is contained in the STR it should not be disseminated to any third party without a prior consent of the person detected the suspicious transaction. Except for these, there are no provisions on protection of the directors, officers and employees of the REs from liability for the reporting of data in good faith to the FAU.

208. *Criterion 21.2* – The prohibition required by this criterion is introduced through Section 38 and 40 of the AML/CFT Act, according to which obliged entities and their employees, employees of FAU and supervisory authorities are prohibited to disclose any information concerning STRs and their analysis. Section 11 of the Labour Code defines directors (governors) and managers as falling under the definition of employee. Sanctions for cases of violation of this provision are set under 43 of the AML/CFT Act.

Weighting and Conclusion

209. There are no explicit provisions in the Czech Republic legislation on protection of the directors, officers and employees of the REs from liability for the reporting of data in good faith to the FAU. **Czech Republic is PC with R.21.**

Recommendation 22 – DNFBPs: Customer due diligence

210. The Czech Republic was rated Partially Compliant with R.12 in its 4th round MER. The evaluators emphasised inability to implement some requirements of the FATF Recommendations (some cascading from the implementation of former R.5, some effectiveness concerns).

211. *Criterion 22.1* – S.2 of the AML/CFT Act defines all DNFBPs with some deficiencies as described below. The identification and CDD requirements of Part 2, Chapter I, AML/CFT Act equally apply to the DNBFPs. CDD weaknesses as identified in R.10 are also relevant for the DNBFPs.

a) Casinos are subject to CDD for transactions amounting to EUR 2,000 or more (S.9(1)(d). Casinos fall under the general definition of gambling operators. Gambling includes internet games, odds betting, live and technical game and more (Act No. 186/2016 on Gambling);

b) Real estate agents are obliged entities and are subject to CDD when trading or brokering with real estate, which includes CDD both for purchasers and vendors of real estate;

c) Dealers of precious stones and dealers of precious metals when they engage in cash transactions which equal or exceed EUR 15,000 are captured by S.2(2)(c) and (d): entrepreneurs when they receive payments of EUR 10,000 or more, or legal persons when they receive payments in cash in an amount of or exceeding EUR 10,000. S.28 AML/CFT Act provides for the CDD requirements for entrepreneurs and legal persons when dealing with a transaction in cash of EUR 10,000 or more. This section basically refers to the other sections of the AML/CFT Act on CDD. There is also a prohibition to accept cash payments exceeding CZK 270,000 (EUR 10,500) (No 254/2004 Sb. on Restriction of Cash Payments);

d) S.2(1)(g) refers to lawyers and public notaries; this section does not cover other independent legal professionals. However, the authorities indicate that these professions will be covered by S.2(1)(h)(5). The definition for lawyers and public notaries refers to representing clients or to act on their behalf; the law does not specify that the services also include preparing for or carrying out transactions concerning the activities in R.22. S.2(1)(e) covers accountants and the law is also applicable to auditors.

e) S.2(1)(h) defines TCSPs as persons that are not lawyers or notaries that provide the listed services as listed in R.22 to another person. The definition does not specify that the services include preparation for or carrying out transactions for a client concerning the activities in R.22. The definition does not include acting as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons and acting as a trustee of an express trust or performing the equivalent function for another form of legal arrangement.

212. *Criterion 22.2* – The record keeping requirements of Part 2, Chapter II, AML/CFT Act also apply to DNBFPs. As described in R.11, there is no clear requirement in the AML/CFT Law for DNFBPs to maintain records on account files, business correspondence and/or results of any relevant analysis and it is not explicitly required to retain the records in a way suitable to reconstruct individual transactions. For casinos and gaming operators S.58(5) and S.60 Act No 186/2016 Coll. On Gambling also have record keeping requirements.

213. *Criterion 22.3* – The PEP requirements of the AML/CFT Act also apply to DNBFPs. Deficiencies in R.12 relate to life insurance and are therefore not relevant for DNFBPs.

214. *Criterion 22.4* – The description under R.15 on new technology requirements equally applies to DNBFPs.

215. *Criterion 22.5* – The description on third party requirements in R.17 also applies to DNBFPs: there is a deficiency with respect to the fact that the information should be obtained immediately and that copies and documentation are made available from the third party upon request without delay.

Weighting and Conclusion

216. Certain weaknesses as identified in R.10 are also relevant for DNBFPs. Deficiencies noted under R.15 (new technologies) and R.17 (third party requirements) apply also to DNFBPs. **Czech Republic is PC with R.22.**

Recommendation 23 – DNFBPs: Other measures

217. The Czech Republic was rated Partially Compliant in its 4th round MER.

218. *Criterion 23.1* – DNBFPs are required to report STRs based on S.18 AML/CFT Act. Therefore, the analysis in R.20 is similarly applicable to DNFBPs. a) Exceptions from this are specified in the provisions for accountants, (S.26(1) and (2)), and lawyers and notaries (S.27(1) and (2)). These provisions provide for the exceptions of professional secrecy and legal privilege. Based on these provisions, lawyers and notaries report STRs to their self-regulatory body, which upon examination of the STR refer it to the FAU. b) With respect to dealers when carrying out a cash transaction above 10,000 EUR, they have in accordance with S.28(e) the obligation to report an STR to the FAU. Even though the Act on Cash Payments provides for a limit to cash payments of 10,000 EUR or more, it is possible that transactions are linked. In this case S.54(4) AML/CFT Act states that if a payment is

divided into several instalments, the value of the transaction shall be the sum of these instalments, provided they are related.

219. *Criterion 23.2* – The description in R.18 applies to DNBFPs. This means that even though many DNFBPs will be small entities, it is unclear from S.22 AML/CFT Act if the compliance officer has to be at management level. Lawyers, notaries and accountants have to introduce and apply adequate policies and procedures of internal control and communication to mitigate and effectively manage ML/FT risks as identified in the risk assessment, but this does not have to be a written system of internal rules, procedures and control measures.

220. Since S.28 AML/CFT Act (entrepreneurs and legal persons when dealing with transaction in cash of EUR 10,000 or more) has no reference to S.21 AML/CFT Act on internal controls, these dealers have no obligation to establish internal control policies and procedures.

221. *Criterion 23.3* – The deficiencies highlighted in R.19 also apply to DNBFPs. Even though obliged entities have to take into account information on high risk countries, there is no requirement to apply EDD. Also, the requirement to apply countermeasures is not clear and explicit.

222. *Criterion 23.4* – The description of R.21 similarly applies to DNBFPs.

Weighting and Conclusion

223. CR is rated PM for the C.23.1 and 23.4 and NM for C.23.3. **Czech Republic is PC with R.23.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

224. In its previous MER, CzR was rated PC with R.33. The shortcomings were the verification of the identity the beneficial owner; lack of in-depth analysis of beneficial owners; existence of bearer shares; inadequate registration of business entities.

225. New legislation dealing with transparency of beneficial owner came into force on 1.1.2017 and into effect on 1.1.2018 at which date the Register on Beneficial Owners was established (S.118b–118j Act on Public Registers). It is not a public register (S.118c), but the relevant authorities and the obliged entities have access to it (S.118g). The deadlines for legal persons registered in the Commercial Register and legal persons registered in other public registers to report to the Register Court data on its beneficial owner is 1.1.2019 for legal persons registered in the Commercial Register and 1.1.2021 for legal persons registered in other public registers (i.e. Register of Associations, the Register of Foundations, Register of Institutes, the Register of Associations of Unit Owners, and the Register of Publicly Beneficial Associations).

226. *Criterion 24.1* – The process for the creation of legal persons is set out in the Civil Code (association S.214, foundation S.306, endowment fund S.394, institute S.402, association of unit owners S.1194) and the Business Corporations Act (unlimited partnership S.95, limited partnership S.118, limited liability company S.132, joint-stock company S.243, cooperative S.552)[83]. Information on the processes for the creation of legal persons is available on the website of the Czech Trade Agency (Ministry of Industry and Trade)[84].

[83] http://obcanskyzakonik.justice.cz/index.php/home/zakony-a-stanoviska/preklady/english.

[84] http://www.businessinfo.cz/cs/clanky/obchodni-korporace-zalozeni-a-vznik-ppbi-50403.html#!&chapter=1

227. The Register on Beneficial Owners is established as of 1.1.2018. Every legal person registered in a public register has to register its beneficial owner in the register. It is not a public register and therefore information on beneficial ownership information is not publicly available.

228. *Criterion 24.2* – The NRA does not assess the risks of all types of legal persons created in CzR, but considers the risks posed by some legal forms (e.g., NPO, offshore structures, complex structures of companies) based on the analysis of actual threats detected. The authorities indicated that an assessment that would be based on mere statistics of all types of legal persons would be perceived as abstract and academic.

229. *Criterion 24.3* – All legal persons are required to be registered in a public register. The registered information includes the company name, legal reason of incorporation, legal form and status, the address of the registered office, basic regulating powers and a list of directors. This is publicly available[85].

230. *Criterion 24.4* – Although there is no requirement for all types of legal persons to maintain information on shareholders itself, there is a requirement to register the information in the public register. Therefore, information about partners of Unlimited Partnerships, Limited Partnerships, and Limited Liability Companies is always visible in the public register either explicitly in the Public Register or indirectly as a mandatory part of the company's Memorandum of Association publicly available in the Collection of Instruments (a part of the Register). Information about the sole shareholder of a Joint-Stock Company is also always public.

231. Limited Liability Companies and Joint-Stock Companies are required to maintain a list of shareholders, number of shares, number of votes (S.139, S.264 Business Corporations Act.). Unlimited Partnerships and Limited Partnerships do not maintain a list of members because the change of a member is only possible by a change of the Memorandum of Association, which therefore always includes the names and other information on members. Cooperatives have to maintain a list of members (S.580 Business Corporations Act). Associations are not obliged to maintain a list of its members.

232. *Criterion 24.5* – S.11(2) Act on the Public Registers requires that the application for registration must be submitted without undue delay after the introduction of a decisive fact. The registrar court is to register the information in the appropriate public register within 5 working days from the day of the delivery of the application (S.96(1)). A change in the information also needs to be registered in the Public Register without undue delay after each relevant event that is causing the necessity of a change of entry. However, as mentioned in 24.4 not all legal persons are required to maintain information on their shareholders or members. In the same time the Act on the Public Registers does not provide any mechanisms or procedure for the Registrar to verify and up-date on a timely basis the information referred to under EC 24.3 and 24.4.

233. *Criterion 24.6* – a, b) All legal persons are obliged to keep and continuously record current data on the identification and verification of the identity of its beneficial owners and to register this in the Register of Information on Beneficial Owners (S.29b(5) AML/CFT Act). S.118d Act on the Public Registers requires registrar courts to maintain in the Register of Beneficial Owners information concerning every registered legal person. The registration of beneficial ownership information is to be submitted without undue delay after each relevant event (S.118e). The registrar court registers the information within 5 working days (S. 118i).

[85] https://or.justice.cz/ias/ui/rejstrik-$firma

c) Additionally, obliged entities are required to obtain and keep information on beneficial owners (see R.10/22).

234. *Criterion 24.7* – All legal persons are obliged to hold current and accurate information on its beneficial ownership. The registrar registers information about the beneficial owner as provided and does not verify the information (S.118h). The Act on Public Registers does not require the registrar to verify the information about the beneficial owner (S.118h) but checks are performed to prevent submission of fake identities. In the same time the Act on the Public Registers does not provide any mechanisms or procedure for the Registrar to verify and up-date on a timely basis the information referred to under EC 24.3 and 24.4.

235. *Criterion 24.8* –S.118e(1) Act on the Public Registers requires an authorised person to submit the application containing beneficial ownership information. This person is generally the person acting on behalf of a legal entity in accordance with the Act on the Public Registers or other acts such as the Civil Code and the Business Corporations Act.

236. *Criterion 24.9* – S29b(3) AML/CFT Act requires a legal person, a trustee or any other person in a similar position in a relation to the legal entity without legal capacity to maintain the information necessary to authenticate the identity of the beneficial owner for the whole duration of the beneficial ownership and for at least additional 10 years after the end of such a relationship. There is no requirement for the legal person (or its administrators, liquidators or other persons involved in the dissolution of the company) to keep the information after its dissolution. Information on dissolution and liquidation of a legal person is to be registered in the public register. According to the authorities, there is no deadline for record keeping in the register after dissolution. Obliged entities have to keep data on beneficial ownership for a period of 10 years after the transaction or termination of business relationship (S.16 AML/CFT Act).

237. *Criterion 24.10* – Access to all public registers containing basic information is available online. Based on the Act on the Public Registers, the competent authorities, including law enforcement authorities, have remote access to the Register on Beneficial Owners. S.29b(5) AML/CFT Act also provides the competent authorities the powers to request from a legal person information about the beneficial owner.

238. *Criterion 24.11* – In accordance with S.263(2) of the Business Corporations Act, a company may issue bearer shares only as book-entry securities or immobilised securities. Bearer shares that have not been immobilised or converted to book-entered bearer shares by 1 January 2014, have been converted into registered shares automatically by force of law.

561. *Criterion 24.12* – Although the Czech law does not provide for the concept of nominees, the legislation does not prohibit a person from acting as a nominee director or shareholder and there is no mechanism to prevent this.

239. *Criterion 24.13* – There are administrative sanctions for not providing or incorrect submission of information to the Public Register. The Registrar Court may impose repeatedly a fine up to 100.000 CZK (EUR 3.775) if a registered person does not inform a registrar court of decisive facts or not submit updated and current documents on the notice of the registrar court (S.9, S.104, S.105 Act on the Public Registers). The registrar court may also make a decision on the dissolution of a legal person with a liquidation in case the person repeatedly does not meet the imposed obligation and as such may cause significant negative consequences for third persons. The law does not imply any direct administrative or criminal liability for legal and/or natural person for incorrect data submission to the Register of Information on Beneficial Owners.

240. *Criterion 24.14* – Access to all public registers containing basic information is available online. The competent authorities can obtain BO information from the Register. The FAU can request from legal entities information on the beneficial owners (S.29b(5) AML/CFT Act). The FAU is the competent authority to cooperate with foreign authorities and international organizations for the purpose of the AML/CFT Act. As described in R37-40, there are some deficiencies but other competent authorities can also exchange information with their foreign counterparts to a large extent.

241. *Criterion 24.15* – The authorities indicated that the FAU monitors the responses and that their quality and accuracy is very different, depending on the legal framework and capacities of the foreign counterparts. However there is no formal mechanism to ensure the quality of the assistance received by the Czech authorities in response to requests for basic and BO information.

Weighting and Conclusion

242. Czech Republic meets or mostly meets majority of criteria, whilst C.24.2, C.24.5, C.24.7 and C.24.13 are partly met. There are public registers with ample information (including on beneficial owners) on all types of legal entities. Although there is no requirement for all types of legal persons to maintain information on shareholders or members, there is a requirement to register the information in the public register. Information on the beneficial owner is recorded in the Register on Beneficial Owners, but it will not be disclosed if it concerns a nominee. There is no direct administrative or criminal liability for legal and/or natural person for incorrect data submission to the Register of Information on Beneficial Owners. The legislation does not prohibit a person from acting as a nominee director or shareholder. There is no mechanism or procedure for the registrar or any other authority to verify and update on a timely basis the beneficial ownership information. There is no requirement for a legal person to keep information after its dissolution. The NRA does not address the risks of all types of legal persons created in the country. **Czech Republic is LC with R.24.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

243. In its 4th round MER, Czech Republic was rated Not-Applicable with R.34. Requirements related to incorporation of trust were significantly changed in 2014. On the 1.1.2014, the concept of trusts has been included in the Civil Code.

244. *Criterion 25.1* – a) Division 4 of the Civil Code on trusts requires that information on the trustee, settlor (founder), beneficiary is recorded, it is implicit that the information is adequate, accurate and current. According to S.65d(e), (g), (h), (i) Act on the Public Registers information on the trustee, settlor(founder), beneficiary and protector has to be registered in the Register of Trusts. b) The legislation does not specify the responsibility for the trustees to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors. c) The legislation also does not specify records retention requirements for professional trustees. Moreover, S.1474 of the Civil Code states that the trustee shall, within thirty days from the termination of a trust, submit an application for deletion of the trust from the evidence of trusts.

245. *Criterion 25.2* – According to S.65b and S.65c Act on the Public Registers the trustee has to submit the registration application on a set up or change or deletion of a record on a trust. According to S.11(2) Act on the Public Registers the competent person is obliged to file a registration application to register a change of information registered in the Register of Trusts without undue delay after each relevant event.

246. *Criterion 25.3* – Every trust in the Czech Republic has to be registered (see EC 25.2) and the Register is publicly available. In addition, the Trusts must register for tax purposes and present documents including on bank accounts. The tax authority verifies the account with the bank. Therefore, even if the trustee did not declare being a trustee, the bank would know this from the request from the tax authority.

247. S.436 and S.1400 Civil Code on general provisions on administration of property of others contains requirements under which the trustee is presumed to make juridical acts as the trusts legal representative and if it is not evident that the trustee acts on behalf of trust, he is conclusively presumed to act in his own name. Therefore, if the trustee needs or wants to act in the name of the trust, he has to disclose his status to the other parties.

248. *Criterion 25.4* – There are no legal impediments preventing professional trustees from providing information referred to under this criterion.

249. *Criterion 25.5* – Competent authorities and obliged entities have access to information in the Register of Trusts and the Registers on Beneficial Ownership. The information includes the beneficial owner, the residence of trustee, and the purpose of the trust. Law enforcement and other competent authorities can also request information from the obliged entities.

250. *Criterion 25.6* – The Trust Register information is available to competent authorities based on the Public Register Act. The FAU is the competent authority to cooperate with foreign authorities and international organizations for the purpose of the AML/CFT Act. As described in R37-40, there are some deficiencies but other competent authorities can also exchange information with their foreign counterparts to a large extent.

251. *Criterion 25.7* – The general provisions of the Civil Code (S.1411 and S.2894) apply under which the trustee will be liable for any harm if he fails to perform his powers and duties with due managerial care. The trustee also has administrative liability (S.9(2) Act No. 251/2016, on some administrative offences), criminal liability (embezzlement S.206 Criminal Code, infringement of the obligations to administer foreign assets (S.220 Criminal Code, infringement of the obligations to administer foreign assets out of negligence S.221 Criminal Code).

252. *Criterion 25.8* – The data related to trusts is available in the Trust Registrar and all competent authorities have access to it. If the record in the Register of Trusts is not in compliance with a binding provision of law and the trustee fails to correct the record, the Registrar Court may repeatedly impose a fine of up to 100.000 CZK (EUR 3.775) or decide to dissolve the trust, if it is in accordance with the interest of third parties. Trustees are obliged to provide truthful and complete information to the Register on Beneficial Owners, but the law does not imply any sanctions for incorrect data submission to the BO Register. According to S 45 of the AML/CFT Law failure to inform the FAU is sanctioned with a fine up to 10,000,000 CZK (377,500 EURO).

Weighting and Conclusion

253. Czech Republic meets the criteria, only C.25.1 is partly met. The legislation does not specify the responsibility for the trustees to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors; and it also does not specify records retention requirements for professional trustees. **Czech Republic is LC with R.25**.

Recommendation 26 – Regulation and supervision of financial institutions

254. In its previous MER, Czech Republic was rated PC with R.23. The following shortcomings were identified: the low number of annual inspections in relation to AML/CFT especially in the banking sector; no clarity as to whether there is a cycle of inspections which catches all financial obliged entities at some point; a very light touch risk-based supervisory approach was taken overall in respect of AML/CFT; the number of obliged entities where infringements were identified as a result of onsite inspection appeared to be low; CFT issues insufficiently addressed in supervision.

255. *Criterion 26.1* – According to S.35 AML/CFT Act the FAU is the supervisory authority performing supervision of compliance with obligations of the AML/CFT Act by the obliged entities. The FAU also controls whether obliged entities do not legitimize the proceeds of crime or finance terrorism. As a result, FAU has a general authorization to supervise all obliged entities. In addition, also according to S.35, CNB supervises the obliged entities under its supervision: the banking sector, the capital market, the insurance industry, pension funds, credit unions, bureaux-de-change and payment institutions (MVTS) for AML/CFT.

256. *Criterion 26.2* – The CNB is responsible for general supervision of the entire financial sector in the Czech Republic (Article 44 Act on the Czech National Bank). The CNB issues authorizations (licenses) to the majority of entities providing services on the financial market (banks, insurance companies, investment firms, management companies, payment institutions as MVTS, money exchange providers). Core Principles financial institutions are obliged to be licensed by the CNB. Licensing requirements are set out in the respective sectoral legislation (Act on Banks, Act on Credit Unions, Capital Market Undertakings Act, Act on Investment Companies and Investment Funds, Insurance Act, Act on Payment Services, Act on Bureau-de-change Activity, Act on Consumer Credit).

257. A range of smaller providers on the Czech financial market is subject to registration procedures which do not allow the entry of a non-fit and proper entity or natural person. Since December 2016, the CNB has received a new competence to license/register non-bank credit providers (the licensing process is currently in course).

258. The Act on Banks contains a set of obligations that banks have to comply with (minimum capital requirements, reporting obligations, corporate governance, risk management, bank management and internal control, meetings of shareholders, registered office, number of employees, etc. (Sections 4, 8, 8a, 8b, 8c, etc. Act on Banks)), therefore shell banks cannot be established or operated in the Czech Republic.

259. *Criterion 26.3* – With several exceptions specified below, the CNB applies a fit and proper test to screen all owners and the members and candidates for the management board, statutory body and supervisory board of the entity/applicant for the license (S.4, S.8, S.16 S.20 Act on Banks; S.2a, S.2b, S.7 Act on Credit Unions; S.6, S.10, S.10b, S10c Capital Market Undertakings Act; S.21, S.479, S.515-516, S.520-522, S.624 Act on Management Companies and Investment Funds; S.7a, S.13, S.24, S.25 Insurance Act; S.9, S.11 Act on Payment Services (MVTS); S.47, S.48, S.52b Act on Payment Services (E-money institutions); S.6, S.8, S.9 Act on Bureau-de-change Activity; S.10, S.72 Act on Consumer Credit).

260. The CNB has also issued various Decrees on applications, approval of persons and the manner to substantiate fit and properness of persons (CNB Decree No. 233/2009 for banks, credit unions and investment firms, CNB Decree No. 247/2013 on Applications for Fund management firms, CNB Decree No. 307/2016 on Applications for Insurance companies, CNB Decree No. 381/2016 on Applications for Non-banking providers of consumer loans). These decrees stipulate the documents and information to be provided on the fitness and propriety of persons holding senior management

functions and qualifying holdings. For the investment firms these are regulated by the directly applicable EU regulations.

261. According to above mentioned documents, the screening is required in case of any market entry into any sector of the Czech financial market. The same screening processes are applied to prevent associates of criminals from holding a significant or controlling interest of financial institution as well as to prevent associates of criminals from being the beneficial owner of financial institution or from holding a management position in a financial institution.

262. For domestic persons, CNB requests an extract from the Criminal Register. Foreign senior managers and persons with qualifying holdings have to provide a document on having no criminal record issued by a foreign (a document similar to an extract from the Criminal Register). Applicants also have to provide information on criminal, administrative or other similar proceedings as well as on closely related persons.

263. For the acquisition of or increase in a qualified holding, the CNB also requests for original counterparts of documents on the origin of the funds from which the acquisition of or increase in a qualified holding is to be financed.

264. With respect to banks, CNB requests an extract from the Criminal Register concerning natural persons who are founders of the bank, who are nominated as members of the statutory body, members of the administrative board and members of the supervisory board of the bank. A person convicted lawfully in the past of a property offence or a criminal offence whose facts relate to banking activities or of a wilful criminal offence committed in connection with business activities may not act as a member of the statutory body, a member of the administrative board or a member of the supervisory board of the bank. The Act on Banks does not provide a requirement to check that criminals are not the beneficial owner of financial institution. Associates of criminals also are not explicitly addressed by the Act on Banks as well as any other regulatory document.

265. Insurance undertakings perform their own fit and proper assessment and notify the CNB about the changes of persons in key function positions. CNB analyses the documentation provided and performs a full ex-post assessment. In case of uncompleted documentation or doubts about the correctness or reliability of the documentation provided, as well as in case of doubts of the appropriateness of the results of insurance undertaking's internal assessments, CNB contacts the insurance company and takes supervisory measures depending on the character of the issue identified.

266. Payment institutions (MVTS), electronic money institutions, bureaux-de-change are obliged to inform the CNB about any criminal record concerning its management (management includes members of statutory body, chief clerk, director or any other person managing the entity) as well as information on any changes regarding members of management including information that allows the CNB to verify if such newly nominated member of management has any criminal record by checking the Criminal Register. For a foreign national an extract from the crime register of his home country (not older than 3 months) has to be provided to the CNB.

267. *Criterion 26.4* –

a) All core principle institutions are subject to the Core Principles, including for AML/CFT. The 2012 FSAP is still actual as the core legislation concerning the regulation, licensing and supervision of banks has not changed substantially since then. The FSAP concluded that as of 2012 compliance with the Basel Core Principles for Effective Banking Supervision had improved markedly since the previous assessment. At the same time, it was concluded that further improvements were needed to achieve all the minimum requirements set by the Core Principles and also to reach the best practices

necessary to increase the resilience of the banking system. An overarching weakness was the insufficiency of staff resources for supervision. This had led to inadequate supervision in several areas, such as too infrequent onsite inspections and delayed remedial action for identified weaknesses in banks. The view of the BCP assessors was that more frequent onsite supervision was required and that the sector of credit unions required more intense supervision[86]. In addition, the recommendations to require credit institutions to have compliance programs, with components for audit, training, and a designated compliance officer(s) at the management level, that address AML/CFT and financial crime, were made. The latter was not addressed by the authorities.

b) All non-core financial institutions, including MVTS, are regulated and supervised for compliance with prudential (where applicable), consumer protection and AML/CFT requirements by the CNB. AML/CFT obligations are also supervised by the FAU. See Crit. 26.1 and 26.2 for details.

268. *Criterion 26.5* (Partly Met) –

CNB

269. Supervision of financial institutions is carried out by 2 departments: Financial Market Supervision Department and Financial Market Supervision Department II. The Financial Market Supervision Department supervises credit institutions, insurance companies and pension companies. The Financial Market Supervision Department II supervises non-banking capital market entities, non-banking credit providers, currency exchange offices, non-banking payment service providers and financial distributors. These two departments work separately (except for general information sharing and cooperation, when appropriate) and their manners of planning and undertaking supervision may (and do) differ.

270. Both departments do not have any approved procedure or regulation which would contain the formal and complete list of criteria used for determining the frequency and intensity of on-site and off-site AML/CFT supervision of financial institution of groups. However, on practice, each department has specific risk assessment system which it uses for the purpose of conducting risk-based AML/CFT supervision. The detailed description of risk assessment system applied by each department is described in Chapter 6, Core Issue 3 on risk-based supervision.

271. CNB`s Financial Market Supervision Department applies a comprehensive AML/CFT risk-based supervision system. The model for determining the frequency and intensity of on-site supervision used by the CNB Financial Market Supervision Department II would benefit from being more AML/CFT driven.

The risk assessment systems of both departments take into consideration the internal policies procedures and controls of the FIs (26.5 (a)). For FMSD I the questionnaire which constitutes the basis for the risk-based supervision is constructed on the findings of the NRA (25.5 (b)) and the characteristics of the financial institutions and groups (26.5 (c). The NRA findings are taken into consideration amongst the factors determining the frequency of the inspections of the FMSD II (26.5 (b)) and the A, B, C categorization was done taking into account the size and other characteristics of the FIs (26.5 (c)).

FAU

[86]https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/en/about_cnb/international_relations/imf_wb/download/fsap_cr_fsap_basel_core_principles.pdf

272. It supervises all obliged entities. In line with the risk-based approach, the FAU takes into account the risk factors specific to an obliged entity. These include, for example, the number of STRs filed, the ownership structure of the customer, the quality and level of communication of the obliged entity in the process of evaluating the system of internal procedures, the volume of business, the way of performing the customer identification (face-to-face, third party). The FAU also takes into account the deficiencies identified by the FAU and the CNB in previous inspections, the risk factors, the characteristic of the obliged entity, the initiatives from the FAU Analytical Division and other national authorities. When planning the inspections, the FAU uses also the outputs from the NRA report, and takes into account the fact that certain types of obliged entities are supervised by other supervisory authorities.

273. The FAU also does not have any approved procedure or regulation which would contain the formal and complete list of criteria used for determining the frequency and intensity of on-site and off-site AML/CFT supervision of financial institution of groups. The used model for determining the frequency and intensity of on-site AML/CFT supervision does not provide any determination of risks for individual institutions at some point of time as well as for determination of ML/FT risks for groups of institutions within particular sectors. FAU`s risk assessment systems partially correspond with the requirements of C. 26.5(a) and 26.5(b) with no indication of C. 26.5(c).

274. CNB and FAU take into account the national risk assessment in their supervisory activities. The CNB's Financial Market Supervision Department planning of AML/CFT inspections is based on self-assessment questionnaire which includes qualitative and quantitative questions on AML/CFT compliance and ML/FT risks. The Financial Market Supervision Department II takes into account of the NRA and the general risks of the currency exchange offices and non-banking payment services providers. This department does not determine the inherent ML/FT risks of an institution.

275. *Criterion 26.6* – The evaluation team was not able to review any formal approved procedure or regulation of FAU or CNB which would provide for periodic review of the ML/FT risk profile of financial institution of groups and when there are major events or developments in the management and operations of the financial institution or group.

276. The CNB indicated that it re-evaluates the overall RAS risk profiles of financial institutions at least once per year. Additionally, the AML/CFT supervision plan is also reviewed and updated once per year. In case of a major event which could affect the risk assessment of a supervised entity or a specific segment of financial market, the CNB indicated that the risk assessment can be reviewed on ad hoc basis and can be reflected in the plan of supervisory activity.

277. The FAU`s used model for determining the frequency and intensity of on-site AML/CFT supervision does not provide any determination of risks for individual institutions at some point of time as well as for determination of ML/FT risks for groups of institutions within particular sectors. Thus, periodic re-evaluation of risks for individual institutions or groups also not possible.

Weighting and Conclusion

278. For some smaller FIs, the CNB has to rely on information provided by these providers. FAU and CNB do not have any formally approved procedures or regulations which would contain the list of criteria used for determining the frequency and intensity of on-site and off-site AML/CFT supervision of financial institution of groups. **Czech Republic is LC with R.26.**

Recommendation 27 – Powers of supervisors

279. In the previous MER, Czech Republic was rated LC with former R.29. The rating was based on no adequate powers of enforcement and sanctions against directors or senior managers of financial institutions for failure to comply with or implement AML/CFT requirements; and it was unclear whether there was a power to sanction for refusal to disclose information to a supervisor.

280. *Criterion 27.1* – S.35 AML/CFT Act appoints the FAU to perform supervision of AML/CFT compliance by the obliged entities and the CNB to supervise AML/CFT compliance with respect of those obliged entities under its supervision. S.15 Act No. 69/2006, on the Implementation of International Sanctions Act (IIS), gives the CNB the power to supervise and ensure the compliance of financial institutions in the area of international sanctions and the FAU for other entities.

281. The CNB conducts financial market supervision on the basis of the authorization laid down in the Act on the CNB. Its supervisory obligations and powers in the financial sectors are set forth in sector-specific acts (S.44, S.45 Act on CNB, S.25 Act on Banks, S.21 Act on Credit Unions, S.135 Capital Market Undertakings Act, S.534 Act on Management Companies and Investment, S.84, S.86 Insurance Act, S.94 Act on Retirement Savings, S.135a Act on Payment Services, S. 17 Act on Bureau-de-change Activity, S. 135 Act on Consumer Credit).

282. *Criterion 27.2* – Inspections of the FAU and the CNB are overall guided by the Act No 255/2012 Coll., Inspection Code, which gives the possibility to enter the premises, check the identity, realize control transactions, request for documents related to the subject of control, make copies of such documents, ask for cooperation of control subjects and others.

283. *Criterion 27.3* – The FAU and the CNB can request access to data from obliged entities for the purposes of undertaking supervision on the basis of the Inspection Code. Based on S.8(c) Inspection Code controllers may request the provision of data, documents and items pertaining to the subject of inspection or activities of the inspected party.

284. *Criterion 27.4* – S.52(1) of the AML/CFT Act gives the power to decide on the offences for non-compliance with AML/CFT requirements to the supervisory body that identifies them (FAU or CNB). The supervisory authority may impose a range of fines depending on the offence (Sections 43 to 50). The fines range from CZK 200,000 (EUR 7,700) to CZK 10,000,000 (EUR 387,000). S.51a of the AML/CFT Act gives the supervisors the power to impose an administrative penalty of the publication of the decision on offence taking into account the nature and the relevance as well as other circumstances of the offence committed.

285. S.36 AML/CFT Act authorises the FAU, should it learn that a legal or a natural person with an income from business or other independent gainful activity has materially, grossly or repeatedly violated any of its obligations under the AML/CFT Act, to lodge a motion to terminate or revoke a license for business or other gainful activity to the authority, which, under another law, has the power to decide on the revocation. In addition, both the FAU and CNB can impose other measures than pecuniary sanctions such as written warnings and orders for remedial measures. Based on S.10(2) Inspection Code, obliged entities have to submit a written report on elimination or prevention of the deficiencies determined by the inspection within the deadline designated by the inspector.

286. However, as indicated in R35, overall level of sanctions is not fully proportionate and not necessarily dissuasive. In addition, the AML/CFT Act does not provide for the sanction of suspending or restricting licenses. It`s also not clear on what management positions sanctions for AML/CFT breaches to individuals can be applied for each sector.

Weighting and Conclusion

287. Czech Republic meets C.27.1, 27.2 and 27.3. C.27.4 is mostly met. There are no sanctions on suspending or restricting licenses. **Czech Republic is LC with R.27.**

Recommendation 28 – Regulation and supervision of DNFBPs

288. In the previous MER, Czech Republic was rated PC with R.24. The rating was based on problematic cooperation between the FIU and the professional chambers regarding AML/CFT supervision; no authority performs inspections on some DNFPB; no sanctions had been imposed; poor understanding regarding financing of terrorism.

289. *Criterion 28.1* –

a) According to S.7(2)(a) Act on Gambling it is forbidden to operate a game for which no license has been issued. This also applies to casino games. The licensing process is split between the Ministry of Finance, that issues the basic license, and the municipal authority, that issues the license for the gambling premises location. There are specific requirements for each application procedure and it is always necessary to obtain the basic license first.

b) The Ministry of Finance is taking necessary legal or regulatory measures to prevent criminals or their associates from holding an interest in a casino. In line with S.6 Act of Gambling the Ministry of Finance investigates the status of the operator (requirements are mainly focused on transparent and clear origin of its resources as well as transparent ownership structure).

290. According to S.91 and 92 Act of Gambling the Ministry of Finance also verifies the individuals related to the applicant – all relevant individuals must prove their free-debt status and the clean record. According to Act of Gambling a person with a clean record shall exclude a person conclusively sentenced for a deliberate criminal offence, or for an economic criminal offence, or for a criminal offence against property, unless such person should be regarded as not sentenced. The Ministry of Finance is responsible to perform necessary actions to support the fact of a clean record of the person.

c) According to S.35(1)(b) AML/CFT Act the "administrative authorities with powers to supervise the compliance with the legislation regulating gambling services in respect of holders of permission for placement of gambling space" carries out supervision of gambling operators including casinos. The Customs Administration is the authorised regulator in the field of gaming since 1 January 2017 in accordance with Act No 186/2016 Coll. The Customs Administration cooperates closely with the FAU on preparation of the scope of the on-sites and the extent and proper understanding of AML/CFT controls.

291. *Criterion 28.2, 28.3* – For DNFBPs, the FAU is the supervisory authority responsible for compliance with the obligations of the AML/CFT Act, with the exception of lawyers and notaries which are supervised by their professional chambers. As described in R.27 the FAU has adequate powers to inspect and powers to issues fines under the AML/CFT Act. .

292. Czech Republic is strengthening a law that grants authorization to real estate agents. Real estate agents will in future have to meet the conditions of professional and personal ability, but this is not yet the case. This law has been proposed by the Ministry for Regional Development and is currently in legislation process.

293. S.37(2) AML/CFT Act states that based on a written initiative from the FAU, the relevant professional chamber shall be obliged to check compliance with the AML/CFT obligations and notify the FAU of the results within the deadline specified.

294. *Criterion 28.4* –

295. Professional licenses are granted to lawyers, auditors, tax advisors, bailiffs, and notaries. In the case of accountants, the professional license is voluntary. For the other DNFBPs, no specific certification is required. According to S.6 of Act No. 455/1991 Coll., the Trade Act, the conditions are authenticity and integrity.

296. **The Czech Bar Association** is a self-governing professional body performing public administration in the area of the Legal Profession. According to S.46 Act No. 85/1996 Coll. on the Legal Profession, the Supervisory Council is responsible to supervise compliance by lawyers. It performs general checks on lawyers in connection with the performance of lawyer's duties regarding lawyer's custody of client's money. This includes review of compliance with lawyer's duties under the AML/CFT Act.

297. The Bar Association is of the opinion that it has sufficient control instruments and sanctions mechanisms available to perform its functions. Administrative penalties include the power of the Bar Association to impose disciplinary sanctions on lawyers – failure to comply with an AML/CFT measure is disciplinary misconduct, as it involves non-compliance with the legal and professional duties. In the draft amendment to the Act on the Legal Profession there is a new disciplinary measure - temporary prohibition on practicing the legal profession in connection with administration of client's property, including interim measures within disciplinary proceedings. The draft amendment was enacted and should come into effect in October 2017 at the latest.

298. Registration in the list of lawyers is conditional, inter alia, on accredited (confirmed by means of an examination) professional qualification and clean criminal record. A person who has been convicted of a crime of whatever nature cannot be registered in the list of lawyers.

299. **The Notarial Chamber of the Czech Republic** is a self-governing professional body which, in the field of AML/CFT, acts as an intermediary between the notary and the concerned authorities. The Notarial Chamber according to Act no. 358/1992 as amended, the Notarial Code conducts inspection of notaries that are members of a local Notarial chamber. There is an AML/CFT component in these inspections. The Chamber has the authority to issue instructions to individual notaries regarding the AML/CFT requirements and other obligations.

300. The Chamber of Notaries established a special disciplinary body called the Disciplinary Commission. There are varieties of sanctions that can be imposed when violations are found. According to S.48 the sanctions that can be imposed are written warning, fine, revocation from office.

301. There are various ways the Notarial Chamber ensures that no criminal becomes a notary or that a person, who is a notary, will not continue in this function, when he or she commits a serious crime. One of the main conditions for becoming a notary is to provide the Chamber with a clean extract from the records of criminal register. Furthermore, S.11 of the Notarial Code states, that the Minister of Justice has the authority to revoke the notary from his or her office when the notary is convicted for intentional criminal offence or criminal offence committed in connection with the notarial activities.

302. *Criterion 28.5* – As described in R.26, the FAU uses a risk-based approach to determine the frequency and intensity of its supervision. The Customs Administration has recently commenced

AML/CFT supervision of the gaming sector and works closely with the FAU in setting up it supervision.

303. The frequency and intensity of lawyers' supervision is set by the Supervisory Council of the Bar Association for each calendar year; checks are performed both in general and ad hoc in specific cases, either based on a complaint or some other external instigation, or on request of the FAU. The AML/CFT aspect is also taken into account when setting the frequency of checks.

304. The frequency of regular controls and checks of notary offices is mandatory, very rigid and very thorough according to the Notarial Chamber. It is an obligation of local Notary Chamber to ensure that each notary and his office are checked every three years.

305. There is no requirement for these SRBs to apply risk-sensitive approaches to supervision. There is no requirement for the SRBs to take into account the degree of discretion allowed to the DNFBPs under the risk-based approach, when assessing the adequacy of AML/CFT internal controls, policies and procedures.

Weighting and Conclusion

306. Czech Republic meets C.28.1. C.28.2, C28.3 and C28.4 are mostly met. C.28.5 is partly met. There are insufficient measures to prevent criminals from being professionally accredited, holding a controlling interest or management function for several DNFBPs. Supervision is not performed on a risk-sensitive basis for casinos, lawyers and notaries. **Czech Republic is LC with R.28**.

Recommendation 29 - Financial intelligence units

307. Czech Republic was rated largely compliant during the 4th round with the former Recommendation 26. This was mainly due to the limitation of the FAU independence with the powers of the Ministry of Finance, as well as overconcentration on tax related issues.

308. *Criterion 29.1* – The FAU, is a national centre for receiving and analysing suspicious transaction reports and for dissemination of the results of the analysis (Section 18 of the AML Act). In addition to STRs, it also receives other types of information, including report from Tax or Customs Administration (Section 30 para.2 of the AML Act), reports from intelligence services (Section 30, par.6 of the AML Act), other motion (Section 55 par.2 of the AML Act).

309. *Criterion 29.2* – The FAU serves as a central agency for the receipt of a) suspicious transaction reports filed by obliged entities as required by R.20 and 23; and, b) other disclosures containing information as required by national legislation. These disclosures include information on suspicious cross-border movements of cash and bearer negotiable instruments (pursuant to Section 41 of the AML/CFT Act) including all cases of violation of this obligation (par.3, Section 42 of the AML/CFT Act).

310. *Criterion 29.3* – a) Section 24 of the AML/CFT Act empowers the FAU to request and use additional information from obliged entities, as needed to perform analysis. Special provisions are stipulated under Section 27 of the AML/CFT Act for lawyers and notaries according to which the FAU can request and obtain such information and documents via the respective Chambers. This provision does not limit the possibility of the FAU to obtain information but it could breach the confidentiality of the cases under investigation. The AML/CFT Law is silent on this issue for other professionals (i.e. Auditors, Tax Advisors, etc.). b) In line with Section 30 of the AML/CFT Act, the FAU is empowered to request and obtain information from LEAs and other public authorities.

311. *Criterion 29.4* –

a) According to Sections 29c, 30 and 31 of the AML/CFT Act the FAU conducts operational analysis of suspicious transactions based on available and obtainable information.

b) There is no requirement in the law for the FAU to undertake strategic analysis, except from Section 30a, which states that the FAU should coordinate the process of the National ML/FT Risk assessment. Apart from typologies used for the NRA purposes no other strategic analyses were undertaken by the FAU.

312. *Criterion 29.5* – According to Section 32 the FAU is authorised to disseminate spontaneously information and the results of its analysis to relevant competent authorities. According to Section 30(6) the FAU shall only notify the intelligence service of the conclusions on the analysis of the suspicious transaction received from latter, while it is silent on sharing information upon request. Hence, while the FAU is empowered to disseminate data spontaneously, its powers for dissemination of information upon request seem to be limited. Information exchange is mainly conducted through protected channel of MoneyWeb data boxes, etc.

313. *Criterion 29.6* – The FAU has an obligation in the course of its activity to apply such organizational, personnel and other measures guaranteeing that an unauthorised person will not come into contact with information gathered during its activity under the AML/CFT Act (Section 29c par.3 of the AML/CFT Act). The FAU should ensure the application of Personal Data Protection Act (Section 31 of the AML/CFT Act). Rules on protection of confidential information in the FAU are stipulated under the Regulation No. 1/2017 of the Director of the FAU. According to Section 38 of the AML/CFT Act employees of the FAU are obliged to keep confidential facts relating to suspicious transaction reports and their investigation, steps taken by the FAU or the obligation to inform under Section 24 of the AML/CFT Act or Section 31c of the AML/CFT Act. Exceptions from confidentiality regime, referring to e.g. disclosure of information to LEAs, supervisors etc., are stipulated in Section 39 of the AM/CFT Act, which are related to sharing information with LEAs and foreign counterparts. b)-c) The rights and obligations of the employees when handling with sensitive and confidential information, and specific measures of physical and administrative security exercised by the FAU are stipulated in the Regulation No. 1/2017 of the Director of the FAU.

314. *Criterion 29.7* – As of 1 January 2017, the FAU has been transformed from the Ministry of Finance divisions, to as a separate "Organizational unit of state" (Section 29c of the AML/CFT Act). The Director of the FAU is appointed by the State Secretary of the Ministry of Finance. The Permanent Commission of the Chamber of Deputies performs the control of the activity of the FAU. The Permanent Commission is not authorised to intervene to the personnel powers of the director of the FAU and to replace its managing competencies (Section 31b of the AML/CFT Act). The FAU has the obligation to submit to the Permanent Commission and to the government an annual report for the last calendar year.

315. The FAU has legally established core functions. Under par.2, Section 29c of the AML/CFT Act, the FAU is authorised to operate in the areas of activities regulated by the AML/CFT Act and by other laws, including decision-making as regards initiating analysis and research, gathering, processing and sharing of information and conducting of controls.

316. The recourses of the FAU are ensured by the Ministry of Finance, however the allocation of them is decided by the FAU itself. The number of FAU staff members is 56.

317. *Criterion 29.8* – The FAU is a member of the Egmont Group of FIUs since 1997.

Weighting and Conclusion

318. The CzR meets most of the requirements under R.29. At the same time the ability of the FAU to conduct strategic analysis is not explicitly covered and no strategic analysis product except from the NRA has been developed by the FAU. Although there are no obstacles in practice, national legislation limits the FAU's ability to respond to the requests sent by the LEAs. **Czech Republic is LC with R.29.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

319. In the MER 2011, Czech Republic was rated partially compliant on requirements or the then R.27. The deficiencies identified were related to few successful police-generated ML investigations, lack of coordinated police – prosecutors' actions and lack of statistics.

320. *Criterion 30.1* – The Police of the CzR is the main law enforcement authority that has the responsibility to investigate ML, FT and associates predicate offences. The following police units are authorised to investigate ML criminal offences: National Unit against Organised Crime (NOCA), National Anti-Drug Unit, Regional Police Directorates and also District Police Directorates. The National Unit against Organised Crime is the nation-wide competence unit combatting organised crime which deals with the most serious cases, e.g. the where the proceeds/damage made exceed 150 000 000 CZK (around EUR 5,860 000.00), and which fall under the jurisdiction of the High Public Prosecutor. If the drug related crime is a predicate offence to ML then the National Anti-Drug Unit may also investigate ML. Regional Police Directorates are dealing with the offences which fall under the competence of the Regional Courts (Section 17 of the CPC) (criminal offences for which the maximum penalty is 5 years of imprisonment). The District Police Directorates investigates crimes under the competence of the District Courts (Section 16 CPC). The terrorist financing offences are investigated by the NOCA (as per the binding instruction of the Police President no. 103/2013) and are prosecuted by the High Public Prosecutor (as per Rules of Procedure of the Public Prosecutor's Office, Regulation No. 226/2016 Coll.).

321. *Criterion 30.2* – The Czech Republic has set up specialised services, both police and prosecutorial to carry out financial investigations. Binding Instruction of the Police President No. 174/2011 "On the Financial Investigation" as amended, regulates the financial investigation and the seizure of proceeds deriving from any criminal offence committed in country or abroad. Section 3 of the Instruction imposes a police officer(s) who carries out the investigation of a crime where property was damaged or where material benefit was gained to thoroughly investigate and secure the proceeds of crime (or their equivalent value) from the moment the investigation has started. For more complex financial investigations, the Instruction foresees engagement of a specialist/expert. The Police have about 210 qualified financial investigators. They are deployed throughout the country and at every level of the police force (on district level, regional level as well as at units with nation-wide competence – NOCA and National Anti-Drug Headquarters) whilst the Binding Instruction 174/2011 presents a kind of guideline on how to carry out the financial investigations. In addition, within the Section of Serious Economic Crime and Corruption of NOCA, the Proceed and Money Laundering Department has been established. The Czech Republic also has the specialised prosecutors and judges dealing with the financial investigations.

322. *Criterion 30.3* – The authorities advised that the Czech Republic police authorities (Police and 'authorised bodies' of Customs, Military Police and of some other specialised agencies - as defined by Section 12 of the CPC) have the responsibility for tracing and identifying the proceeds of crime. However, the CPC does not provide a clear definition of the financial investigation neither

designates specific law enforcement authority to 'trace and identify' the proceeds of crime. Nevertheless, Section 79a of the CPC states that the authorities competent to seize the property that is suspected of being the proceeds and instruments of crime, are the chairing judge and the state prosecutor. Police authority is also a competent authority within the meaning of this criterion, however it needs prior consent from prosecutor to seize the property that is suspected to be of a criminal origin. In urgent cases police can act without prior consent by the prosecutor, however the consent must be provided within the 48 hours period.

323. *Criterion 30.4* – The Security Information Service, the Office for Foreign Relations and Military Intelligence which powers are regulated in the Act on Intelligence Services of the Czech Republic (Act no. 153/1994 Coll.) are not law enforcement authorities *per se* but are authorised to obtain the information which is subject to bank secrecy based on the prior consent of the High Court. (Section 8, par 3).

324. The FAU is other non-LEA which has a significant impact on the pursuing of financial investigation, by firstly obtaining relevant information (Section 30 AML/CFT Act), processing such information (Section 31 AML/CFT Act), providing it to internal (Section 32 AML/CFT Act) and external (Section 33 AML/CFT Act) competent LEA.

325. *Criterion 30.5* – The Czech Republic does not have a separate anti-corruption law enforcement authority designated to investigate ML/FT offences arising from, or related to, corruption offences.

Weighting and Conclusion

326. Czech Republic meets all the criteria of this Recommendation apart from criterion 30.3 which is mostly met and for the reason that the CPC does not provide a clear definition of the financial investigation neither designates specific law enforcement authority to 'trace and identify' the proceeds of crime, although the code states that the chairing judge and the state prosecutor are competent to seize criminal assets and instrumentalities. **Czech Republic is LC with R.30.**

Recommendation 31 - Powers of law enforcement and investigative authorities

327. The Czech Republic was rated compliant with regard to former Recommendation 28. This recommendation has been further expanded by introducing requirements for countries to have mechanism in place to identify whether natural or legal person hold or control accounts, and to ensure that competent authorities have a process to identify assets without prior notification to the owner.

328. *Criterion 31.1* – Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing are able to obtain access to all necessary documents and information and use them in these investigations.

a) Section 8 (1) of the CPC provides that the authorities, legal entities and natural persons are obliged to comply with request of authorities involved in criminal proceedings while performing their tasks. Furthermore, s. 8(2) gives powers to the public prosecutor and the presiding judge (after filing an indictment or a motion for punishment) to request *an information subject to banking secrecy, data from the register of investment instruments and booked securities, tax related data and any statistical data.* S 150(3) authorises LEAs to secure the necessary documents, in particular files and other written material in the course of criminal investigation.

b) Search of persons and premises is regulated under Subdivision V of the CPC. The chairing judge (and during the pre-trial proceeding the judge), upon a request of the state prosecutor, is entitled to order the search of premises. The presiding judge and, during the pre-trial proceedings the public prosecutor or police, are entitled to order a search of a person(s).

c) Subdivision II of the CPC regulates taking witness statements by police or public prosecutor.

d) Police and prosecutor have also power to seize and obtain evidence. Sections 78 and 79 of the CPC foresees that anyone who is in position of an object/item which may serve as an evidence is obliged to hand it over it upon a request of the court, state prosecutor or police authority; If the object/item that may serve for evidentiary purposes is not handed over by the person who has it in his/her possession, such an item may be seized upon an order of the presiding judge, and in pre-trial proceedings upon an order of the public prosecutor or police authority. Police must have a previous consent by the public prosecutor for issuing such an order unless for the reasons or urgency the consent by the prosecutor cannot be secured immediately.

329. *Criterion 31.2* – The competent authorities may use a wide range of investigative techniques to investigate ML, associated predicative offences and FT. Those technics include:

a) undercover operations which may have a form of a simulated transfer (Section 158c CPC) and a surveillance of persons and items (Section 158d (2) CPC), both subject to the written authorisation of the prosecutor, are applicable to all crimes committed internationally regardless their level seriousness. The use of an agent (Section 158e CPC) as well as (b) the interception and recording of telecommunications (Section 88 of the CPC) are both subject to approval by a judge and can be used in criminal proceedings for crimes for which i) the law prescribes a minimum sentence of 8 years of imprisonment, ii) the crime the Czech Republic is bound to prosecute in accordance with the international treaties ratified by the country (e.g. ML and FT fall under this criterion), or iii) some specific crimes listed in the law (e.g. economic and organised crimes).

b) Obtaining traffic and location data generated by using electronic communications (Section 88a CPC) is subject to judicial approval and can be used for all premeditated crimes punishable by minimum three years' of imprisonment. S 158 (3) d) of the CPC refers to technical devices (which include computer system according to the authorities interpretation) and approves access to them and their surveillance in the course of criminal investigation, upon judge's approval.

c) Subdivision IV of the CPC regulates interception and opening of consignments, their replacement and monitoring, this being the CzR terminology for what is considered as controlled delivery. These techniques are applicable to all premeditated crimes regardless of their seriousness whilst its application has to be approved by the presiding judge and, during the pre-trial proceedings, by the public prosecutor.

330. *Criterion 31.3* –

a) Competent authorities have mechanism in place to identify whether natural or legal person holds or controls accounts, and to identify assets without prior notification to the owner. The Section 8 Sub-Section 2 of the CPC lays down that a public prosecutor is entitled in the pre-trial proceedings to request a bank information and information about investment instruments in order to identify the nature, extent or the location of objects/items that might be subject(s) to seizure. Moreover, the new Act on Bank Accounts Register which takes effect as of 2018, states *that those authorised to receive information on bank accounts under other laws* (e.g. CPC) shall receive the data form the Central Register of Accounts run by the Czech National Bank no later than 24 hours from the submission of the request.

b) Authorities advised that police have direct access to car and boats registers, whilst indirect access (through the liaison officers of the entities concerned) is granted to databases of personal ID cards/passports, real estate register, register of natural persons conducting business, register of business entities engaged in transportation business, etc. With regard to the requirement to have a process in place to identify the assets without prior notification to the owner, the law remains silent on the issue. Nevertheless, the authorities advised that as long as the law does not explicitly requires police to notify the owner, such measure would not be necessary. In addition, the authorities advised that, in practice, such notification has not been made in any of the cases carried out so far.

331. *Criterion 31.4* – S.39 par.1(a) of the AML/CFT Act read in conjunction with S.8 (1) of the CPC provides authority for the police and prosecutors to request all relevant information from the FAU.

Weighting and Conclusion

332. **Czech Republic is C with R.31**.

Recommendation 32 – Cash Couriers

333. Czech Republic was rated largely compliant with the former FATF Special Recommendation IX whilst certain concerns regarding its effective implementation were raised (mainly low number of ML cases generated by the Customs compared to the criminal activity context of the Czech Republic).

334. *Criterion 32.1* – Czech Republic has implemented a declaration system for incoming and outgoing cross border transportation of currency and bearer negotiable instruments (BNIs), including remittance of cash, as cargo or by post. This was done through implementation of the EU Regulation 1889/2005 and provisions under Section 41 par.1-4 of the AML/CFT Act. However, this declaration system applies only to movements (both inward and outward) of cash and BNI from and to the European Union (extra-Communitarian), meaning that only movements that cross the external borders of the European Union are subject to the declaration requirements. Movements of cash and BNI within the European Union (intra-Communitarian) are not considered to be cross-border movements under the Czech legislation and are not subject to any declaration/disclosure obligation. The declaration requirements in place apply to different modes of transportation.

335. *Criterion 32.2* – By virtue of Section 41 of the AML/CFT Act implementing the EU Regulation no. 1889/2005, the Czech authorities a written declaration system. The obligation to declare applies to any natural person entering or leaving the EU and carrying amounts equal to or larger than EUR 10.000. The declaration obligation applies also to legal person or natural person who acts as an entrepreneur exporting or importing *cash, travel cheques or money orders convertible into cash, bearer or registered securities or any other investment instruments which are signed, but do not contain the name of the recipient, in the value of EUR 10,000 or higher.* No declaration system exists for movement of funds or for transportation of cash via mail or cargo within the European Union.

336. *Criterion 32.3* – This criterion is not applicable to the Czech Republic as it operates a declaration system.

337. *Criterion 32.4* – Customs authorities supervise the compliance with the obligation to declare currency or BNIs (Section 42 par.1 of the AML/CFT Act). The AML/CFT Act makes no special distinction between a false declaration and a failure to declare. According to the Act on Customs Administration (No 17/2012 Coll., as amended) customs officers have the right to check natural persons, their baggage and their means of transportation, postal and other shipments (Section 35). They also have a power to require all information and documents they deem relevant (Section 58 par. 5).

338. *Criterion 32.5* – A person fails to meet the obligation to declare, as set out in Article 3 of the EU Regulation 1889/2005, if the information provided is incorrect or incomplete. According to the Section 50 of the AML/CFT Act a person who fails to comply with the obligation is subject to a fine up to CZK 10,000,000 (around 386.000 €) or a forfeiture of the item(s). In case of a serious violation, a criminal proceeding on ML under (Articles 216 and 217 of the CC) has to be launched. The range of penalty for Article 217 CC is up to 3 years or 1-5 years for aggravating circumstances. See c. 3.9 for the penalties for Article 216.

339. *Criterion 32.6* – As required by Article 5 of the EC Regulation 1889/2005, all information obtained by customs through the EC declaration system is provided to the FAU. Pursuant to Section 42(3) of the AML/CFT Act, the customs authorities are required to immediately forward to the FAU *information concerning the compliance with the obligation to declare, including all cases of violation of this obligation*.

340. *Criterion 32.7* – The authorities advised that there is a sufficient level of coordination between the customs and the FAU. The legal basis for such cooperation is embedded in Section 42(3) of the AML/CFT. The exchange of information between the Customs Administration and Police which also carries out the function of the immigration authority is regulated by the Acts on Customs Administration (Act No 17/2012 Coll., as amended), on Police (Act No 273/2008 Coll., as amended) and on Residence of Foreign Nationals on the Territory of the Czech Republic (Act No. 326/1999 Coll. Section 163). The cooperation between the two was formalised through the Cooperation Agreement signed in February 2014 and afterwards amended.

341. *Criterion 32.8* – The customs authority, upon detection of a violation of obligations to declare cross-border cash transit set out in Section 41 of the AML/CFT Act, may freeze items concerned by the violation (Section 42 (4-5) of the AML/CFT Act). The authorities did not however, provide any regulation/norm that would require customs to stop or restrain currency of BNIs for a reasonable time in order to ascertain whether there is a suspicion that ML/FT or predicate offences were committed.

342. *Criterion 32.9* – The general requirement for exchange of information among EU countries and third countries is regulated by Articles 6 and 7 of the Regulation 1889/2005/EC, which is directly binding to all MS. Moreover, Section 33 (1) of the AML/CFT ACT provides basis for FAU international cooperation, including information exchange on cash declarations and transits. As a member of EU, the Czech Republic also applies Regulation 515/97/EC on mutual assistance in customs matters. The rules and the terms of retention of information on declarations, including a false declaration are set by the Customs Administration based on the Act No. 499/2004 Coll., on archive and file management (Section 66 par.1 and 2).

343. *Criterion 32.10* – As the member of the EU, the Czech Republic has to apply safeguards to the personal data privacy which is ensured under the Art. 8 of the Regulation (EC) no 1889/2005. Any disclosure or communication of information shall fully comply with prevailing data protection provisions, in particular Regulation (EC) no 45/2001. As an EU MS, Czech Republic respects the EU's principle of free movement of capital - the Preamble 1 of the EU Regulation 1889/2005 states that the *European Community endeavours to create a space without internal borders in which the free movement of goods, persons, services, and capital is ensured.*

344. *Criterion 32.11* – Authorities advised that the persons carrying out a physical transportation of currency or BNI related to ML/FT or predicate offences would be subjects to proportionate, effective and dissuasive criminal sanctions, referred in art.216 and 217 of the CC (see R.3). The CPC regulates the seizure and confiscation of currency or BNIs (see R.4). However, the limited scope of

the obligation to declare cross-border movement of cash and BNI identified at C.32.1 impacts the compliance with the standards.

Weighting and Conclusion

345. The regime on cross-border transportation of currency and other financial instruments suffers from certain shortcoming - the declaration system does not apply to movements of BNI and cash within the EU. Authorities did not provide any regulation which would enable customs to stop or restrain currency of BNIs for a reasonable time in order to ascertain whether there is a suspicion that ML/FT or predicate offences. **Czech Republic is PC with R.32**.

Recommendation 33 – Statistics

346. The Czech Republic was rated partially compliant with regard to the former R.32. The bases for rating were mainly related to difficulties in providing updated statistics which suggested that they were not available in a timely manner.

347. *Criterion 33.1* – The Czech Republic maintains the following statistical data on matters relevant to the effectiveness and efficiency of their AML/CFT systems:

a) The FAU has a system to routinely maintain statistics on the STRs received and disseminated. This obligation is provided by Art.13 and 18 of the AML/CFT Law (registration and analysis of STRs). Statistics are maintained for each reporting sector and include some characteristics of STRs, such as use of cash. FAU Order No.37/2014 also provide for maintenance of statistics on actions taken following the receipt of STRs, namely the results of pre-trial investigation; court decisions taken in relation to criminal proceedings, and the number of persons who have committed criminal offences or suspected of committing and convicted of crimes. More precisely, the statistical data on STRs, collected by the FAU, provides information on:

- total number of STRs;
- type of obliged entity which files the STR;
- the potential ML/FT technique included in STR;
- result of analysis (including the possible predicate offence in case of criminal complaints;
- number of STRs resulted in dissemination to other institutions;
- requests for information sent/received and to which countries;
- number spontaneous information received.

b) The authorities advised that the Police is in charge to keep statistics on ML/FT investigations; whilst the prosecution service keeps statistics on ML/FT prosecutions and convictions. Ministry of Justice is responsible for gathering statistics from courts and prosecution offices in line with S.7 paragraph & Act no 89 1995 on the State Statistical Service.

c) The FAU holds data on postponed transactions, seizures of funds and number of criminal complaints lodged to the law enforcement authority.

According to the Binding Instruction 174/2011 (section 7 paragraph 1 letter a) and 2 letter d), the Police must keep statistics on actions in financial investigation and statistics on seized property. Such data are gathered within the ETR information system, which enables the collection of statistical data resulting from criminal proceeding conducted by the Police. The investigating officer who executed the seizure orders is obliged to record all the details in the ETR, including the overall

damage caused by the offence. The ETR contains approximately 20 search criteria, such as the type of crime, investigating unit and seized values. The authorities advised that after receiving information on confiscation of property, the police officer shall fill in data on the value of confiscations but the regulatory act this was not provided to the assessment team.

d) MLA or other international requests for cooperation made and received:

The FAU collects statistical data on the numbers of international requests received and sent, cross-border reports received and sent, spontaneous information exchange (received and sent).

There is no centralised case management system available in the Czech Republic. Currently there is a new system of electronic file registry under construction at the Supreme Public Prosecutors (ELVIZ) which will allow collection, compilation and analysis of data on international judicial cooperation at the state level. The system is expected to become operational in 2020. At the moment, the authorities are unable to provide accurate statistics of international cooperation including the types of requests, timeliness of responses, prioritisation of requests or cases of spontaneous dissemination.

Weighting and Conclusion

348. In comparison to information provided in the 2011 MER, the Czech Republic partly rectified the key deficiencies regarding statistics collection. However, ML statistics are not segregated by types of cases (stand-alone ML, self-laundering), and no information on the follow-up of FAUs postponement orders. The authorities do not keep accurate statistics on confiscation, MLAs or other international requests for cooperation received. **Czech Republic is PC with R.33**.

Recommendation 34 – Guidance and feedback

349. The Czech Republic was rated as Partially Compliant in the 4th round of MER. The evaluators found out that there were insufficient guidelines on AML/CFT techniques and methods; insufficient sector specific guidelines, and insufficient specific feedback. The FATF standard has not been changed, but some amendment have been made to the applicable law, and new guidelines have been issued.

350. *Criterion 34.1* – There is no formal obligation for the authorities to provide guidelines to the obliged entities but in practice the FAU and some of the SRBs (The Notarial Chamber, Chamber of Auditors and Tax Advisors) have developed guidelines to the FIs and the respective DNFBPs. Namely, the FAU has issued six Methodological Guidelines on key AML/CFT areas– PEPs, beneficial ownership, virtual currencies, FT and international sanctions (up-dated), submission of STRs and gambling. The guidelines are published on the FAU website.

351. According to the authorities, the FAU and the CNB regularly update their web sites and distribute emails to the FIs and DNBFPs with relevant information on ML/FT trends, best available practices. The CNB regularly publishes on their website the Guidance issued by the European Supervisory Authorities[87] as well as FAQs on the effective application of the general AML/CFT requirements. Ad-hoc guidance is provided on the occasions of the meetings between the FAU and the professional associations (*i.a. Commission of the Czech Banking Association*) and by responding to individual questions from reporting entities should they have doubt regarding the implementation of their AML/CFT obligations. Sector-specific guidelines are not available.

[87] Joint Guidelines of EU 2015/849 on simplified and enhanced CDD and the factors to be considered when assessing the ML and TF risk

352. The AML Act stipulates directly in Section 55 para. 3 that after conclusion of the analyses, the FAU provides feedback to the obliged entities reporting suspicious transaction. The feedback includes information on filed criminal complaints, information sent to other competent authorities or the foreign FIU, and cases shelved in the FAU information system for possible future use. This feedback is general, without disclosing any detailed information.

353. CNB, in particular, its Financial Market Supervision Department, provide regular feedbacks to their supervised entities on the results of the AML/CFT supervisory activity. CNB also publishes FAQs on its website which are general compilation of most relevant AML/CFT obligations.

Weighting and Conclusion

354. The FAU has a legal obligation to provide feedback to obliged entities with regards to the STRs and has provided extensive guidance to financial institutions, and DNFBPs, especially with respect to ML/FT risks and the reporting of suspicious transactions. The guidance provided to the FIs is complemented by the EU Guidance and FAQs issued by CNB. There is no legal obligation to provide guidance. **Czech Republic is LC with the R.34.**

Recommendation 35 – Sanctions

355. In its 2010 MER, Czech Republic was rated PC with R.17. The rating was based on (1) Administrative sanctions included within the AML/CFT Law are not proportionate and not necessarily dissuasive, as the maximum financial sanctions that can be applied are quite low; (2) Except for violation of the obligation of confidentiality, on which administrative fines may be imposed on natural persons, all the other administrative penalties can only be imposed on legal obliged entities. Directors, managers and employees are not directly sanctionable; (3) · No financial sanctions have been applied (effectiveness issue).

356. *Criterion 35.1*– The AML/CFT Law provides for administrative sanctions applicable to both FIs and DNFBPs in the event of breaches of AML/CFT requirements with the exceptions described below.

357. Breaches related to the application of third party and introducers rules are indirectly and partially covered through the sanctions applicable for failure to perform CDD. However, not all the requirements of R 19 are such sanctionable (*i.a.* c. 17.1.c)

358. Administrative sanctions related to breach of obligation related to the targeted international sanctions on terrorism and terrorist financing are stipulated in the Act on Implementation of International Sanctions, Part 5 (R 6).

359. To regulate the sanctioning regime in case of breaches related to R8, Section 104 of the PRA Act articulates that, in case of violation, the register courts may impose repeatedly a fine up to 100 000 CZK/EUR 3,877. In case of repeated failure to fulfill this obligation, if there is a legal interest therein and if it can have serious consequences for third parties, the Registry Court may, under Section 105 of the PRA, initiate proceedings on the cancellation of the registered person with liquidation. The shortcomings described under c. 8.5 apply.

360. The range of fines that are stipulated by the law are set out in the following table.

Table 23: administrative fines for Breach of AML/CFT Law

AML/CFT Law	Administrative fines (up to)	If breach makes it more difficult to identify or seize the proceeds of crime, or make the financing of

			terrorism possible (up to)	
	CZK	**€ ***	**CZK**	**€ ***
Sect. 43 Violation of the confidentiality	200,000	7,500	1,000,000	37,000
Sect. 44 CDD	up to 1,000,000 or up to 10,000,000 depending on a failure	up to 37,000 or up to 370,500 depending on a failure	None (as of 2010 MER was 50,000,000)	None
Sect. 45 Failure to respond to FIU request	10,000,000	370,500	None (as of 2010 MER was 50,000,000)	None
Sect. 46 Failure to report STR	5,000,000	185,000	None (as of 2010 MER was 50,000,000)	None
Sect. 47 Failure to suspend the Transaction	up to 1,000,000 or up to 10,000,000 depending on a failure	up to 37,000 or up to 370,500 depending on a failure	None (as of 2010 MER was 50,000,000)	None
Sect. 48 Failure to comply with other preventive obligations (e.g. internal rules, training, etc.)	up to 1,000,000 or up to 5,000,000 depending on a failure	up to 37,000 or up to 185,000 depending on a failure	None (as of 2010 MER was 50,000,000)	None
Sect. 49 Failure to comply with wire transfer regulation			None (as of 2010 MER was 50,000,000)	None
Sect. 50 Cross border disclosure	10,000,000	370,500	None (as of 2010 MER was 50,000,000)	None

361. In a view of the assessment team the administrative sanctions included within the AML/CFT Law are not proportionate and not necessarily dissuasive. The maximum level of sanctions provided by AML/CFT Law is up to CZK 10,000,000 (~ EUR 370,500) is not dissuasive enough.

362. After the 2011 MER, the sanctions provided in Sections 44 – 50 of the AML/CFT Act were weakened (a fine of CZK 50,000,000/EUR 1,938,622 is no longer possible) for cases when breach of the AML/CFT Act would make it more difficult to identify or seize the proceeds of crime, or make the financing of terrorism possible. To this, the Czech Authorities explained that corroborated, the changes in legislation only harshened the sanctioning regime. With the adoption of Act 418/2011 Coll. on Criminal Liability of Legal Persons, the sanctions are calculated on a "daily rate" which can vary from CZK 1.000 to CZK 2.000.000 (EUR 38.77 to EUR 77,543). The daily rate is determined by the court, taking into account the financial situation of the legal person. The Criminal Code then stipulates in its Section 68 para. 1 that the maximum number of days which can be imposed on legal person is 730 which means that the highest fine can reach CZK 1.460.000.000/EUR 56,606,704. When determining the number of days imposed to the legal person, the Court takes into consideration the nature and seriousness of the committed criminal offence. However, these sanctions can be applied only in the course of a criminal procedure and are not available for administrative breaches.

363. According to Section 51a of the AML/CFT Act, a breach of the obligations stipulated under Section 43 - 49 of the AML/CFT Act, may also entail a penalty of publication of the sanctioning decision on the FAU website for a period of 5 years. The information would be circulated in the form of "news" notice which will be sent to all registered visitors of the FAU website. The Czech authorities advised that in practice such instrument has not been used yet, due to short period since

its adoption, corroborated with the duration of administrative proceedings (including the appealing instruments).

364. The limitation period of offenses is 3 years and begins to run on the day following the day of the offense.

365. According to Section 53 of the AML/CFT Act, sanctions for breach of obligations by legal and advisory professionals (except accountants) are applied by the professional chambers on the basis of disciplinary powers given in special laws. If other supervisory authority finds violations of AML/CFT Act by legal professionals, the matter will be referred to the competent professional chamber.

Financial Sector

366. Starting 1st January 2017 the CNB can now also apply pecuniary sanctions for AML/CFT breaches based directly on the AML/CFT Act. FAU and CNB have similar powers to impose sanctions which can be applied to same categories of financial institutions..

367. The CNB can apply non-pecuniary sanctions for breaches of AML/CFT obligations based on the general authorisation given in the various sectorial laws governing the different sectors of the financial market[88].

368. Non-pecuniary sanctions available to the CNB based on sectorial legislation consist of, amongst others:

- requirement to change the management of the institution,
- modify the conditions of the license (i.e. by restricting permitted activities),
- order an exceptional audit,
- revoke the license and others.

DNFBPs

369. FAU has a general authorisation to supervise and impose sanctions to the DNFBPs other than legal and advisory professions[89].

According to Section 53 of the AML/CFT Act, sanctions for breach of obligations by legal and advisory professionals (except accountants) are applied by the professional chambers on the basis of disciplinary powers given in special laws. If other supervisory authority finds violations of AML/CFT Act by legal professionals, the matter will be referred to the competent professional chamber.

370. Notary Chamber of the Czech Republic can apply number of sanctions when violations are found.

[88] Sector specific provisions concerning the financial sector: Banks - Section 26 para 6 of the Act on Banks; Credit unions - Section 28 para 2 and Section 28g of the Act on Credit Unions; Investment firms – Section 136 of the Capital Market Undertakings Act, Section 9 and 9b of the Law on Supervision in the Capital Market (No. 15/1998 Coll.); Fund management companies - Section 539 of the Act on Management Companies and Investment Funds, Section 9 and 9b of the Law on Supervision in the Capital Market (No. 15/1998 Coll.); Insurance companies - Section 95 of the Insurance Act; MVTSPs and e-money institutions - Section 135d of the Act on Payment System; Exchange bureaus - Section 18 and 19 of the Act on Bureau-de-change Activity; Non-banking providers of loans - Section 146 of the Act on Consumer Credit.

[89] Accountants are supervised by the FAU although they are a part of legal and advisory professions.

371. As a result of violation, disciplinary proceedings can be initiated and when the notary is found guilty, mainly three different sanctions can be imposed (regulated by the Notarial Code).

372. According to Section 48 three different sanctions can be imposed on Notary: written warning, fine - up to one hundred of the minimum monthly salary[90] or a revoked from office. The amount is different for Notaries, Notary associates and Notary Trainees. The maximum fine for Notaries can be up to CZK 1.220.000 (EUR 47,301), the maximum fine for Notary Associates can be up to CZK 244.000 (EUR 9,462) and the maximum fine for Notary Trainee can be up to CZK 61.000 (EUR 2,365).

373. There are two main sanctions that can be imposed on Associate and on trainee associate:

- associate - written warning and/or a fine up to twenty times the monthly salary
- trainee associate - written warning and/or a fine up to five times the monthly salary.

374. The Chamber of Tax Advisors pursuant to Section 12 and 13 of the Act No. 523/1992 Coll may impose on the tax adviser the following disciplinary measures:

- written reprimand,
- fine up to an amount of CZK 100,000 (EUR 3,878),
- suspension of provision of tax advisory services for as long as one year,
- deletion from the List.

375. Czech Bar Association can apply following disciplinary sanctions for lawyers when violations are found:

- an admonition,
- a public admonition,
- a fine of up to one hundred times the monthly minimum wage set by special legislation
- a temporary ban on practicing the legal profession imposed for a period of six months up to three years,
- termination of membership in the Bar by striking name off the Register of Lawyers (Act on the Legal Profession - section 32 paragraph 3)

376. The Bailiffs' Chamber may submit a disciplinary action (complaint) against bailiff to Supreme Administrative Court (disciplinary body) for significant breaching of duties stipulated by legal (e.g. AML/CFT Act) or professional regulation (e.g. lack of cooperation during supervision, Sections 116,117 and 121 Act No. 120/2001 Coll., on bailiff and executory activities).

377. In accordance with Section 25 of Act No. 93/2009 Coll., on Auditors, for the breach of obligations the Chamber of Auditors of the Czech Republic may impose following:

- Admonition
- Public admonition
- Fine up to CZK 1,000,000, and in certain cases up to CZK 10,000,000 (approx. EUR 40,000 and EUR 400,000)
- Prohibition of activity for the period up to 5 years

[90] The Czech authorities advised that the minimum monthly salary is of CZK 12.200.

- Exclusion from performance of a member of the governing body of audit company for the period of maximum 3 years.

378. *Criterion 35.2* – According to sections 43-50 of the AML/CFT Law, the administrative sanctions to natural persons can be applied only for violation of the obligation of confidentiality (Section 43) and failure to comply with the obligation to declare during a cross-border transport of cash (Section 50)).

379. The Czech Authorities informed that the liability for the administrative offence for natural persons was adjusted in the Act No. 250/2016 on offences and proceedings, in Section 13 for natural persons and Section 20 for legal persons. According to Section 20 par.7 of the Act, the liability of legal person does not exclude the possibility to impose the sanction to the natural person as well. The evaluation team was not provided with mentioned regulatory changes nor with confirmation that such sanctions have been imposed on natural persons. It was unclear to what management levels sanctions for AML/CFT breaches can be applied for each sector.

Weighting and Conclusion

380. Overall, sanctions for AML/CFT breaches have limited proportionality. The range of sanctions applicable to natural persons for AML/CFT breaches is limited and the available administrative sanctions are not dissuasive enough, as the maximum financial sanctions that can be applied are quite low. **Czech Republic is PC with the R.35.**

Recommendation 36 – International instruments

381. In the MER 2006, the Czech Republic was rated PC for both former R.35 and former SRI. It was noted that the country had ratified neither the Palermo Convention nor the Convention against Terrorist Financing. Reference was made to the deficiencies regarding the freezing of funds in response to the UNSCRs. At the time of the last follow-up report, these issues had not been resolved. In the interim, however, the Czech Republic ratified all the relevant conventions, including the UNCAC, which has since become a requirement under new R. 36.

382. *Criterion 36.1* – Czechoslovakia signed the Vienna Convention on 7 December 1989 and ratified it on 4 June 1991 (the Czech Republic acceded on 20 December 1993). The Palermo Convention (UNTOC) and its two Protocols (Protocol against the Smuggling of Migrants by Land, Sea and Air and Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition) entered into force on 24 October 2013.

383. The Merida Convention (UNCAC) entered into force on 29 December 2013. The Merida Convention was domestically published as No. 105/2013 Coll. of International treaties, while the Terrorist Financing Convention entered into force on January 26, 2006.

384. Under Czech Constitution (Article 10) the promulgated treaties, the ratification of which Parliament has given its consent and by which the Czech Republic is bound, form a part of the legal system; if a treaty provides something other than that which a statute provides, the treaty shall apply. Thus all four treaties are directly applicable and shall take precedence over statute and therefore fully implemented.

385. *Criterion 36.2* – The Czech Republic has substantially implemented the relevant treaties, though there still are minor deficiencies in relation to the ML and FT offences. In addition, the

treaties require that signatories be equipped to provide MLA, inter alia, in relation to freezing, seizing and confiscation. As discussed under R. 38, there are minor deficiencies in this regard.

Weighting and Conclusion

386. While the CzR has ratified and brought into force the Palermo, Mérida and Terrorist Financing Conventions, evidence of their full implementation appears still to be lacking. **The Czech Republic is LC with R.36**.

Recommendation 37 - Mutual legal assistance

387. At the time of the MER 2006, the CzR was rated LC for former R. 36-38 and former SR V. The assessors noted that there was some concern about the CzR's ability to provide timely and effective assistance in view of apparent limitations in relation to R.37 (regarding indirect proceeds and value confiscation) and the situation with the resources devoted to the area of MLA. At the time of the 4th follow-up report in 2011, little had changed in terms of legal provisions in this area, but since that time, the Czech Republic has brought into force a new statute dealing with MLA.

388. *Criterion 37.1* – The Czech Republic has Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters (hereinafter IJCCM). The Act has been in force since 1 January 2014.

389. The new Act appears to be the result, in part, of an attempt by CzR authorities to shorten the Criminal Procedure Code, bearing in mind the voluminous passages that transpose European Directives and other regulations into Czech law. Nevertheless, the Act, which contains 358 sections, is quite complete and sets forth a number of means of assistance that the CzR is capable of providing at S. 47. The list includes:

> Legal assistance consisting in:
>
> a) Surrender and Removal of Items, Seizure of Financial Resources, Booked Securities, Real Estate and other Asset Values (pursuant to Chapter IV, Sub-division four of the Criminal Procedure Code Sections 78-81b),
>
> b) House and Personal Search, Search of Other Premises and Parcels, Entry to Residence, Other Premises and Parcels (Chapter IV, Sub-division five of the Criminal Procedure Code Sections 82-85c),
>
> c) securing the claim of an aggrieved person pursuant to Chapter II, Sub-division seven of the CPC, d) intercepting and opening consignments and its replacement (pursuant to Chapter IV, Sub-division six of the CPC),
>
> e) monitoring consignments (which is the term used in Czech legislation for "Controlled Delivery) Pursuant to Section 65 of the IJCCM
>
> f) interception and recording of telecommunications pursuant to Chapter IV, Sub-division seven of the CPC, this investigative technique would only be available for ML in the most serious of circumstances (s. 216(4), s. 214(4)s.), though not for FT, because of the requirement that the offence be punishable by imprisonment for 8 years or more.
>
> g) inspection of mental state pursuant to Section 116 (2) of the CPC,
>
> h) use of operative-search means pursuant to Section 158b to 158 f of the CPC, or
>
> i) covert investigation pursuant to Section 59 to 61, S. 50 of the IJCCM which deals with the procedure for taking statements from witnesses and experts, while S. 51 governs the

presence and participation (if authorised, foreign authorities may ask additional questions to the witness).

Under S. 57 and 58 of the IJCCM, provision is made for a foreign state to request an interview/witness statement via video-conference or via telephone.

j) Interception and recording of telecommunications can be ordered by court in these criminal proceedings:

- Concerning all crimes (no connection of the level of sentence) where the CzR is obligated to prosecute them based on international treaty (including ML and financing of terrorism cases);
- Crimes listed in Sec 88(1) of the CPP (no connection to the level of sentence);
- In other cases of intentional crimes where the upper level of the imprisonment is at least 8 years.

390. In terms of the manner of execution of a given request, under Section 3 IJCCM, the authorities proceed according to the CPC unless the IJCCM stipulates otherwise (the IJCCM has to take into consideration the international aspects of cooperation). CzR authorities indicate that if there is an applicable and binding international treaty that stipulates clearly otherwise, the authorities proceed according such a treaty (see Article 10 of the Constitution of the CzR and Section 3/2 IJCCM).

391. The CzR is able to provide a very broad range of mutual legal assistance (hereinafter MLA) in criminal matters including MLA in criminal matters concerning money laundering, associated predicate offences and terrorist financing investigations, prosecutions and related proceedings. A number of measures are available on the basis of reciprocity. The statutory regime contains all necessary measures to provide assistance in a timely manner. Requests are handled on the basis of urgency where such urgency is justified in the request.

392. International judicial cooperation between the Czech Republic and a foreign state can be provided either by an international treaty, or based on the guarantee of reciprocity (see Section 4 IJCCM). Assistance based on reciprocity is very broad, covering virtually the entire range of assistance, though with a few exceptions, such cross-border surveillance. CzR has signed and ratified the major UN, Council of Europe (though the CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime and on the Financing of Terrorism (the 2005, "Warsaw" Convention) has yet to be signed or ratified) and European Union conventions and has implemented all EU legislation concerning MLA in criminal matters but the European investigation order (the bill of implementing law is waiting for approval in the Parliament).

393. While the CzR has at its disposal a wide selection of tools to assist other countries, the minor deficiencies identified in relation to R. 3 and R. 5 can limit the scope of the assistance available because of the requirement of dual criminality for coercive measures.

394. *Criterion 37.2* – In cases where there is pre-trial proceeding being conducted in a foreign state, either by a police or judicial authority, the Supreme Public Prosecutor's Office (hereinafter the SPPO) will be competent to accept a request of the foreign authority for legal assistance as a central authority; otherwise the Ministry of Justice will be competent (S. 48/1 IJCCM). Some information is available to foreign authorities in this regard, either via the Czech Republic's declarations made in relation to the ratification of its treaties, or via the European Judicial Network's website. As a matter of policy, CzR authorities have more recently concentrated the execution of MLA requests in the pre-

trial proceedings at the level of regional public prosecutor´s offices. Other types of requests are handled at the level of regional courts (S. 48/5 JICCM).

395. The CzR is able to provide assistance in a timely manner in cases where the MLA request received is complete and accurate. The execution of MLAs is supervised by the central authorities unless there is an international treaty which allows for a direct contact between judicial authorities (Article 48/3 IJCCM). Authorities advised that most requests in relation to EU countries are executed based on direct contact between judicial authorities in Czech Republic and abroad.

396. Each public prosecutor´s office has its own searchable electronic case management system that allows individual cases to be followed. However, these regional systems are not interlinked between them or linked with the central authorities (PPO and Ministry of Justice). A new case management system (ELVIZ) is in the process of being developed, but is not yet operational.

397. There are templates for use in relation to outgoing requests prepared for Czech prosecutors and judges for all types of MLA and other requests (they are available on Extranet of the SPPO for prosecutors and on Extranet of Ministry of Justice for judges). While the mechanisms by which requests are routed and processed are fairly clear, and while there is a type of case-management system at the regional level, the lack of a central case-management system would presumably prevent authorities from tracking the processing of requests and impede the ability for CzR officials to form an overall view of how well and quickly MLA requests are in fact being executed in order to adjust policies as the case may be to achieve greater effectiveness.

398. *Criterion 37.3* – Under S. 5, a request may be refused if its execution would violate a constitutional principle or negatively impact an essential security interest. S.53 of the IJCCM provides that execution of a foreign request may be suspended if it imperils a CzR investigation and S. 54 covers grounds of refusal (insufficient grounds provided, execution impossible under Czech law, other serious reasons). "Other serious reasons" may include, for example requests whose execution would cause significant damage or would be practically impossible to execute, e.g. finding the body of a person who has been dead for several years without a precise location provided. There would therefore seem to be no unreasonable or unduly restrictive conditions placed on MLA.

399. *Criterion 37.4* –

a) There are no legal provisions which would prohibit the execution of an MLA concerning fiscal offences. On the contrary, the CzR is a party to a number of international treaties (or their additional protocols) and the EU legislation stipulating the obligation for the CzR to provide MLA also for fiscal matters.

b) The IJCCM does not restrict the execution of MLAs on the basis of secrecy or confidentiality requirements, aside from lawyer´s duty of confidentiality and legal professional privileges (S. 8.5 CPC). "Banking secrecy" is not a ground for refusal of the MLA request.

The grounds of refusal or suspension are stated above under Criterion 37.3.

400. *Criterion 37.5* – Section 6 of the IJCCM adequately protects confidentiality of the MLA request. It is noted that CzR pre-trial proceedings are not public. The MLA request is not provided to accused persons or their lawyers. This is true for both pre-trial proceedings (where such notification could have grave consequences if it were an obligation) and trial proceedings in the requesting state.

401. *Criterion 37.6* – Non coercive measure do not require dual criminality, for example, the taking of a statement from a witness, suspects, accused persons; providing bank information (without freezing a bank account); providing a copy of a defendant's criminal conviction record; handing over procedural documents.

402. *Criterion 37.7* – Dual criminality does appear to be assessed on a purposive basis, i.e., that the CzR looks at whether the conduct described in the request would form the basis for a criminal proceeding in the CzR for any criminal offence, regardless of nomenclature or the "category" of offence in question. The addition of tax crimes to the glossary list of designated categories of offences does not affect this dual criminality analysis and consequently does not hamper the CzR's ability to provide assistance for either tax crimes as a predicate or ML based on this newly designated predicate category.

403. *Criterion 37.8* – The standard requires that the powers listed in C.31.1 are available to foreign states based on a valid request for MLA. As set forth above in the analysis of C.37.1, these powers are put at the disposal of the requesting state as required (provided the request complies with the requirements of the relevant treaty or of the IJCCM). As for the powers referred to in C.31.2 and in 37.8 (b) a range of such powers are available on behalf of foreign state. Some of these powers are referred to specifically in C.31.2, but this does not exclude other powers under C.37.8.

a) The powers and investigative techniques mentioned in R.31 are available for executing of MLAs (provided the MLA complies with conditions set by relevant international treaties and/or JICCM). Under Section 12/10 of the CPC the proceedings according to the IJCCM will be understood as criminal proceedings. Under Section 3 IJCCM, the authorities proceed according to the CPC unless the IJCCM stipulates otherwise. However, if the international treaty binding upon the CzR stipulates clearly otherwise, the authorities proceed according such a treaty (see Article 10 of the Constitution of the CzR and Section 3/2 IJCCM).

b) CzR powers to contribute to an undercover operation are referred to at S. 59-61 ("covert investigations") of the IJCCM and the ability to carry out a "controlled delivery" is authorised and regulated in section 87b of the Code of Criminal Procedure and section 65 of the IJCCM. The prosecutor can order the surveillance of a consignment if it is suspected that it contains drugs, false money, arms etc. Simulated transfer (fictive transfer) is covered in section 158c of the Code of Criminal Procedure and section 61-63 of IJCCM. This means, for example, a simulated transfer of forged money, drugs etc. and it is done by an undercover agent or a person who cooperates with police authority.

The interception of communication is available and can be used if a criminal proceeding is conducted for a crime, for which the law prescribes a sentence of imprisonment with the upper limit of at least eight years, or for crimes listed in Section 88(1) of the CPC or for crimes which the Czech Republic has the duty to prosecute according international treaties (i.e. money laundering). In effect this means that the interception of communication can be used in any case of investigation of money laundering. In addition, Czech law authorizes taking of statements via video-conferencing.

It seems clear that some of the treaties or other agreements signed and ratified by the CzR provide for direct cooperation between foreign judicial authorities and its own. This matter is dealt with in this Annex under c. 40.1Authorities involved in criminal proceedings proceed in the execution of MLA according to the law of the requesting state – see Section 49 IJCCM.

Weighting and Conclusion

404. The CzR is able to provide a broad range of assistance. While the particular treaties signed and ratified by the CzR provide detail about the specific forms of assistance that may be provided by the CzR, most forms of assistance can be obtained on the basis of reciprocity. However given certain minor deficiencies identified under R. 3 and R. 5, the ability to cooperate fully in relation to these

offences is not entirely demonstrated. Czech authorities do not currently have a complete and centralised case-management system. **The Czech Republic is LC with R. 37**.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

405. At the time of the MER 2006, the Palermo and CFT conventions had not been ratified. It was also noted that the inability for the CzR to go forward with freezing and confiscation of property of equivalent value constituted an additional shortcoming. The report from the 4th Follow-up visit in 2011 reiterated some of these concerns but noted favourably that the problem related to property of equivalent value had been resolved by means of an amendment.

406. *Criterion 38.1* – The authorities initially advised that, in accordance with S. 3/1 IJCCM, the prosecutor or court is authorised to proceed pursuant to the IJCCM unless this Act stipulates otherwise or in cases where it does not regulate a certain issue, CPC will apply. They later added that international treaties can also fill the gap. CzR authorities point out that the prosecutor or court "*can directly apply also a self-executing provision of the international treaty that was ratified by the CzR and published in its Collection of Law or the Collection of International Treaties* (see Section 3/2 of the IJCCM – 'Procedure according to this Act will apply, unless an international treaty stipulates otherwise'). CzR authorities have indicated that in fact the CC does apply to some extent to international cooperation. For example, via s. 70(e)(a) of the CC, ss. 77b(1)(b), 79(a), 79(g), the seizure of instrumentalities and property of equivalent value are covered. As for confiscation, s. 118 of the IJCCM is a general provision that authorises the recognition and execution of foreign court orders made in criminal cases. The definition of a foreign decision under s.118 IJCCM is broad, encompassing different types of criminal penalties and protective measures. The definition also covers confiscation and forfeiture orders. It is defined by law as a decision issued by a foreign authority in connection with a criminal offence, by virtue of which a criminal punishment or a protective measure was imposed, as defined in light of CC s. 36, 52, 98(1). Criminal punishments of confiscation of assets under s. 66 CC and confiscation of an item (s. 70-72 CC) and also protective measures of forfeiture of an item (s. 101-102 CC fall within the IJCCM s. 118 definition as well.

407. Overall, in line with the legislation, the Czech authorities look first to the provisions of the IJCCM. If there is no coverage there, they look to the provisions of the CPC. In terms of the precise procedural manner in which the foreign request is to be executed, the terms of the treaty will prevail over the IJCCM or the CPC.

408. The CzR has also implemented Framework Decision 2003/577/SVV on European freezing order (S. 226 -236 of the IJCCM), though this legislation can be used only vis-a-vis the EU Member States that have already implemented this framework.

Subcriteria (a)(b)(c)(d)

409. Section 79 (letter a to g) of the CPC provides the principal authority for and governs details regarding the seizure of laundered property and various other types of property, including instrumentalities and property of equivalent (corresponding) value. Instrumentalities are defined in the Section 70(2)(a) of the CC as an item that was used to commit a criminal act or intended to commit a criminal act. As far as the procedural law is concerned, instrumentalities are defined in Section 77b(1)(b) of the CPC – "(1) An item important for criminal proceedings is an item, which ... b) was intended or used to commit a crime (hereinafter referred to as "instrument of criminal activity")". The concept "instrument of criminal activity" is used with the same meaning in the text of provisions of Section 79a to Section 79g of the CPC.

The IJMCC refers to countries other than the Czech Republic itself either as "Members" (EU Member states) or "foreign" states (all other countries). In terms of confiscation, there is a regime set out in s. 278-295 which is available on the basis of a foreign order, but this applies only to EU members. Sections 278-295 of IJCCM are specific provisions with respect to EU countries that have already implemented the Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (OJ L 328, 24/11/2006 p. 59 – 78).

410. Extended confiscation is covered by Section 102a of CC. Czech authorities advise that in these circumstances, reference may in fact be made to the Criminal Code because any temporary seizure carried out according to the CPC (or according to the CPC and the IJCCM in the case of MLA) can be done only if there is a particular purpose defined by substantive or procedural law.

411. *Criterion 38.2* – The recognition and execution of foreign NCB (non-conviction based) forfeiture can only be done when the foreign state has a similar concept of NCB forfeiture in criminal proceedings (i.e. Slovakia) Czech authorities refer, in this respect, to a current practical example of such a request where the matter is pending before the court. The case involves a confiscation order where one accused is deceased and the other acquitted. Czech authorities advise (although the matter is still pending) that in these circumstances confiscation of money on bank accounts as proceeds of crime can in fact be carried out under s. 101(2)(b)(e) of the CC (via s. 118 of the IJCCM). It is not clear, in any event how a non-conviction based order where a suspect has fled, died or cannot be identified (for example a "civil confiscation" order made in rem vis-à-vis the property of an unknown presumed offender).

412. *Criterion 38.3* – In relation to sub-criterion (a), Czech authorities refer to s. 48/6 of the IJCCM, but this provision deals with the apportionment of the execution of a foreign requests within the Czech Republic amongst prosecutors in various regions of the country. The authorities explain that s. 48(6) of the IJCCM is in fact important in cases of coordination of execution of MLA requests including the coordination of seizure and confiscation actions. For example where several Public Prosecutors (PPO) or courts are competent to execute the MLA request, the MLA request will be executed by only one PPO or court, to which the request was forwarded by the SPPO or the Ministry of Justice. This PPO will then coordinate seizure of assets throughout the country and with appropriate foreign countries. This is an adequate though not ideal response to the requirements of this sub-criterion.

413. In complex cases, the assistance of Eurojust can be required. Eurojust can organize coordination meetings and later to coordinate house searches or asset seizures on international level. Assistance from CARIN can also be requested.

414. Regarding sub-criterion (b), the management of the temporarily seized assets is dealt with under Act No. 279/2003 Coll. dated 7 August 2003 on enforcement of seizure of assets and items in criminal proceedings, *inter alia*.

415. The measures outlined in the analysis under c. 4.4 are available for the purposes of managing assets on behalf of foreign authorities.

416. *Criterion 38.4* – Asset sharing is authorised for the CzR based on the reciprocity (S. 135, 140 IJCCM). Asset sharing is regulated also by the bilateral treaties (in fact there has been one bilateral treaty with the US signed so far). If the cooperation between EU Member States is based on the 2006/783/JHA Framework Decision on confiscation orders, asset sharing is possible (S. 290 of the IJCCM), which can only be used vis-a-vis the EU Member States that have already implemented this framework decision.

Weighting and Conclusion

417. The CzR has the ability to carry out the principal requirements of this recommendation and a robust regime for the management of seized assets is in place. Less complete ability is demonstrated, however, in relation to assisting a requesting country with non-conviction based confiscation. **The Czech Republic is LC with R. 38**

Recommendation 39 – Extradition

418. For reasons that are not clear to the assessors, former R. 38 was not assessed in the MER 2006 and not dealt with in the 4th Follow-up report.

419. *Criterion 39.1* – Extradition to a foreign state is governed by the IJCCM; Extradition to the member states of the European Union, i. e. surrender based on the concept of the European Arrest Warrant, is governed by Sections 189 to 225 of the IJCCM. Extradition to other states is governed by Sections 87 to 104 of the IJCCM.

a) For both Non-EU and EU countries, the issue of whether an offence is extraditable is determined by the length of the maximum sentence (essentially 1 year under Czech law) in relation to the offence for which the person is sought. In both cases, the offences FT and certainly some ML offences are extraditable, but under s. 216 and 214, if the underlying offence is punished by a lesser term of imprisonment, the sentence for ML will be considered in terms of this lesser penalty.

b) While the CzR does not have an electronic case management system, under the EU Arrest Warrant scheme, there are time limits fixed by law (60 days for a decision, S. 209 IJCCM) and the procedure is far simpler than with other countries. With these other countries, the case management system would be an advantage or even an important consideration in case there is a large number of extradition requests, which is not the case. These latter requests are dealt with based on the urgency as justified in the request.

c) Grounds for refusal of extradition are stated in S. 91 for non-EU states. Although they do include the need for a reciprocal agreement when extradition is requested based on a tax or customs offence, this is not in itself unreasonably restrictive. Grounds for refusal are much more limited when extradition is requested by EU Member states, but there may be refusal if a Czech citizen or permanent resident refuses to accept extradition in circumstances where the purpose of the extradition is for execution of a sentence imposed in the requesting state and it is a sentence that may be executed in the CzR instead (S. 205 IJCCM). This is not considered unreasonably restrictive.

420. *Criterion 39.2* –

a) The CzR will refuse to extradite their nationals to a non-EU country unless they consent (S. 91(1)(a) IJCCM), however bilateral treaties on extradition might derogate from this principle. To date, the CzR has no treaties in force which would apply this exception. However, under the concept of the European Arrest Warrant surrender of a Czech national even without his/her consent is possible if specified conditions are met.

b) b) S. 113 (1 and 3) – 117 in conjunction with S.9 of the IJCCM If the CzR refuses surrender based solely on the issue of nationality, CzR authorities state that the matter will immediately be transferred by the Ministry of Justice to a prosecutor for the institution of proceedings For an EU state, it appears that the only basis upon which extradition of a citizen or permanent resident of the CzR may be refused (S.205 of the IJCCM, aside from the lack of necessary information/evidence/material) is that the person sought can serve the sentence imposed in the

other state, in the CzR instead. Therefore the issue raised in 39.2 (b) does not really arise for EU members.

421. *Criterion 39.3* – CzR authorities submitted material including copies of two extradition treaties and references to Czech jurisprudence that confirm that dual criminality will be assessed in line with the FATF standard as stated in the criterion.

422. *Criterion 39.4* – There are provisions in the IJCCM for simplified extradition (S. 96 for non-EU countries, S. 208 for EU countries).

Weighting and Conclusion

423. The CzR is able to extradite for ML and FT based on the maximum sentence for these offences and does not impose overly restrictive conditions on surrender. This is at the heart of R. 39. When refusal of surrender is based solely on nationality, it is possible for CzR authorities to take the matter before a CzR court. However there does not seem to be an obligation to do so at the request of the foreign state. This deficiency can be considered minor. Neither the dual criminality analysis nor the issue of simplified extradition present a problem. **The Czech Republic is LC with R. 39**.

Recommendation 40 – Other forms of international cooperation

424. The Czech Republic was rated LC in the previous round of evaluations. The identified deficiencies were: lack of mechanisms in place for Police and supervisory authorities for collecting data and providing statistics on international cooperation; and need for the FAU to develop a much more detailed process and procedures to keep the information collected on requested cases.

425. *Criterion 40. 1* –

FAU

426. For the FAU there is authority to exchange information (including documents), including classified information as defined by the AML/CFT Act, with foreign financial intelligence bodies (Sections 33 and 39). The exchange of information with foreign authorities is conducted both spontaneously and upon request (for detailed information see Criterion 40.9). This authority extends also to indirect (mostly via foreign FIU) exchange of information with other foreign authorities competent in the field of combating ML/FT (for detailed information see Criterion 40.20).

NOCA

427. Act No. 273/2008 Coll. on the Police of the Czech Republic, namely Sections 89-94 provide the legal basis for international police cooperation. According Section 89, when executing their tasks the Police shall cooperate with Interpol, Europol, relevant authorities and institutions of the European Union and its Member States, as well as with other international organisations, foreign security forces and other competent foreign entities. Sections 90-93 specifically authorize Czech police and foreign counterparts to participate in cross-border operations on the basis of an agreement. S. 94 specifically provides authority for the sharing of information relating to National Security.

428. CzR authorities advised that communication via the Interpol channel was common and widely used. Interpol National Central Bureau ("NCB", Interpol Prague) is located within the Police Presidium and it operates as a central authority for Interpol and other international cooperation/communication. Czech police do provide information spontaneously in the context of European organisations and within joint investigation teams.

Prosecutors

429. Spontaneous information is provided in writing or exchanged during meetings between domestic and foreign prosecutors (often during coordination meetings organised by Eurojust or within the framework of joint investigation teams).

CNB

430. There are no impediments in the international cooperation at the supervisors' level. For more details the reader is referred to EC 40.12 and following.

431. However, the "rapid" provision of the "widest range" of international cooperation is not specifically provided for.

432. *Criterion 40.2 – Competent authorities should*

(a) have a lawful basis for providing co-operation

FAU

433. As indicated under Criterion 40.1, the AML/CFT Act authorizes the FAU to cooperate with foreign authorities. The provisions of the Act are broad enough to allow flexible cooperation.

NOCA

434. As mentioned in 40.1, Act on the Police provides for the legal basis of the international police cooperation. See Section 89, 90, 91, 92, 93 and 94 of the Act on Police.

Prosecutors

435. The Law on International Judicial Cooperation in Criminal Matters sets out the legal basis for cooperation between domestic and foreign prosecutors.

CNB

436. There are legal basis for the CNB international cooperation. For more details the reader is referred to c. 40.12 and following.

(b) be authorised to use the most efficient means to co-operate;

FAU

437. Cooperation is conducted based on the principle of reciprocity or based on an MOU when required by the counterpart authorities' legislation. These means are efficient.

NOCA

438. Police of the Czech Republic are involved in various topic-oriented practitioners´ networks on EU as well as at the global level. These networks enable the exchange of both operational and strategic information, depending on the circumstances. For ML cases in particular, the investigating officer may take advantage of the involvement of the police in the ARO and CARIN networks (focused on the identification of proceeds of crime), EPAC network (network focused on combating corruption), StAR Initiative (recovery of stolen assets) and various Focal Points under Europol.

Prosecutors

439. The Supreme Public Prosecutor´s office issued a cooperation methodology for prosecutors and courts. The Methodology is published on the Extranet in a structural form (templates, guidance, lists of treaties, lists of declarations etc.) and it is accessible to all prosecutors but not public.

Coordination of MLA can be provided also by Eurojust, and specialised networks (the EJN, CARIN ...). These means are considered to be efficient.

CNB

440. The CNB is authorised to use efficient means to co-operate. For more details the reader is referred to c. 40.12 and following.

(c) have clear and secure gateways, mechanisms or channels that will facilitate and allow for the transmission and execution of requests;

FAU

441. Cooperation is provided via the ESW and FIU.Net gateways.

NOCA

442. Interpol requests are processed via I-24/7 (secure global police network) which is installed at NCB Prague (National Central Bureau). The system enables authorised users to share sensitive and urgent police information with their counterparts.

443. Europol requests are processed via SIENA, the Europol's Secure Information Exchange Network Application, which allows LEA to share operational and strategic crime-related information and intelligence via a secure communication channel.

Prosecutors

444. Cooperation between domestic and foreign prosecutors takes place via Eurojust platform.

CNB

445. The CNB does not report using special secure channels.

(d) have clear processes for the prioritisation and timely execution of requests; and

FAU

446. According to the FAU's Methodological Instruction 8 (MI 8), requests are to be processed depending on the scope of required information. Normal requests are to be responded no later than in 20 days; for urgent requests the time limit is 5 days (unless the response is not required immediately).

NOCA

447. The prioritisation and execution processes are regulated by:

- Binding instruction (standard operating procedure) of the Police president No 78/2009 on the activities of NCB Prague (as for Interpol requests);
- Binding instruction (standard operating procedure) of the Police president No 183/2011 on the cooperation with Europol (as for Europol requests);
- Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (as for ARO requests exchanges under Council Decision 2007/845/JHA concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime).

Prosecutors

448. There are certain rules for MLA request prioritisation set out by the Instruction No. 10/2013 issued by the Prosecutor General. These measures are binging for the prosecutors.

CNB

449. No information on prioritization of foreign requests has been provided by the CNB.

(e) have clear processes for safeguarding the information received.

FAU

450. Any dissemination of information to the third party is performed only after the prior written consent of the provider. The information provided to the requesting FIUs shall always be of the same quality and the same scope as information gathered for the FAU's own analysis (MI 8).

NOCA

451. General rules on processing information such as personal data are set forth in Art. 79 – 88 of the Act on the Police. All data received via international police cooperation are processed in the ETR system, the Czech Police´s case management system. The users have various access rights depending on their role. A log –tracking ensures further protection.

Prosecutors

452. Confidentiality of information exchange is regulated by Section 6 of the IJCCM and the respective provisions of the MoUs signed with foreign counterparts.

CNB

453. Information exchange and confidentiality in communication between the CNB and the respective foreign supervisory authorities are regulated through the MOUs signed, in line with Article 2 of the Act on CNB.

454. *Criterion 40.3* –

FAU

455. The FAU cooperates with foreign counterparts based on the principle of reciprocity or based on a MoU whenever is required by the counterpart. To date the FAU has signed total of 31 MoUs.

NOCA

456. Bilateral and multilateral cooperation agreements are the competence of the Police Presidium, International Police Cooperation Department, and Strategic Division, which maintains the list of applicable agreements.

Prosecutors

Bilateral and multilateral cooperation agreements (e.g. to set up a Joint Investigation Team) can be initiated by the Supreme Public Prosecutor's Office according to Section 71of the IJCCM.

CNB

457. As Described under c. 40.12 and following the CNB is able to conclude bilateral and multilateral MoUs.

458. There are no positive regulations indicating that the MoUs should be negotiated and signed in a timely way.

459. *Criterion 40.4* –

FAU

460. Given its Egmont Group membership, the feedback on the use of data and outcomes of the analysis is provided by the FAU to the foreign authority upon request (in line with the Clause 19 of the Egmont Group Principles[91]). There is no indication that this should be done in a "timely manner".

OTHER AUTHORITIES

461. Regarding the other competent authorities, there are no specific legal provisions regulating explicitly the provision of feedback to the authority from which assistance was sought and providing this in a timely manner. However, there are no provisions which would pose an obstacle to doing so. Feedback can be provided to foreign counter-parts unless this violates the general terms of cooperation (see also sub criterion 40.5 (c)).

462. *Criterion 40.5* –

ALL AUTHORITIES

463. No disproportionate or unduly restrictive conditions are applied in the Czech Republic, including on fiscal matters. Exchange of information in the scope of international police cooperation is subject to conditions set by relevant international treaties and/or by relevant provisions of the Act on the Police of the Czech Republic, Criminal Procedural Code and the Act on International Judicial Cooperation.

464. The applicable legislation does not restrict cooperation concerning secrecy or confidentiality requirements (except for lawyers' duty of confidentiality pursuant to the Act on the Legal Profession - Article 8 of the Criminal Procedural Code). The execution of such a request depends on relevant international treaty or reciprocity.

465. According to the international cooperation bilateral treaties, each of the Contracting Parties may refuse, wholly or partly, a request for support should it believe that granting the same might threaten its sovereignty, security or another vital interest, or if it contravened its national legislation or its international obligations. In order to grant the request, the requested Contracting Party may stipulate conditions by which the requesting Contracting Party shall be bound.

466. If the requesting subject is one of those authorised to request / obtain information as per particular treaty on police international cooperation, the requested information will be provided irrespective of the nature or status of the requesting counterpart.

467. *Criterion 40.6* –

468. Based on MI 8, the information provided by foreign counter-parts to FAU should be used for purposes specified by the provider only. The information provided to the requesting FIUs shall always be of the same quality and the same scope as information gathered for the FAU own analysis. Information is shared via secure channels (ESW, FIU.Net).

469. Concerning international police cooperation, information and documents may be provided to third States and international organizations only with a written consent of the transmitting Contracting Party; and by using the information systems established under the EU Laws, for the purposes of cooperation in protecting public order and security as well as fight against crime, in particular the Schengen Information System.

470. *Criterion 40.7* –

[91] Egmont Group of Financial Intelligence Units Principles for Information Exchange Between Financial Intelligence Units.

471. The confidentiality requirements the FAU is bound to are provided under Section 38 of the AML/CFT Act and MI 8. The information obtained on the basis of international cooperation is protected the same way as information received for the purposes of analysis domestically.

472. Czech authorities provided detailed information on the usual content of the bilateral treaties on international police cooperation and how they adequately cover the personal data protection.

473. *Criterion 40.8* – The FAU is authorised to exchange all information required to be accessible or obtainable directly or indirectly by the FIU (see R.29), and any other information which it has the power to obtain or access, directly or indirectly, at the domestic level, subject to the principles of reciprocity. Police of the Czech Republic are able to provide their foreign counterparts with the same scope of information that they use for their own inquiries.

Exchange of Information between FIUs

474. *Criterion 40.9* – Cooperation between FIUs with foreign authorities is regulated by Sections 33 and 39 of the AML/CFT Act and Clause 9 and 11 of the Egmont Group Principles. The FAU is authorised to cooperate with foreign FIUs regardless of their type (e.g. administrative, law enforcement and judicial or other in nature) authorities based on an international treaty or on the principle of reciprocity.

475. *Criterion 40.10* – As a member of the Egmont Group the FAU provides a feedback to its foreign counterparts in accordance with the Clause 19 of the Egmont Group Principles.

476. *Criterion 40.11* –The FAU is authorised to exchange all information required to be accessible or obtainable directly or indirectly by the FAU (under R.29), and any other information which has the power to obtain or access, directly or indirectly, at the domestic level, subject to the principles of reciprocity (AML/CFT Act, Articles 33 and 39(1)(c). There are no provisions set in law or other acts limiting the FAUs ability to do so.

Exchange of Information between financial supervisors

477. *Criterion 40.12* – According to Section 2 par.3 of the Act on CNB, the Czech National Bank can cooperate and negotiate agreements (Memoranda of Understanding) within the scope of its fields of competence with the central banks of other countries, with foreign authorities engaged in financial market supervision, foreign resolution authorities, international financial organisations and international organisations engaged in financial market supervision. The CNB so far concluded between CNB 21 bilateral and 4 multilateral MoUs. As advised by Czech authorities, in general, the MoU include the exchange of information for AML/CFT supervisory purposes.

478. *Criterion 40.13* – Specific provisions governing in detail exchange of information within the EU are set out in the sectoral legislation, concerning in particular exchange of information in cases of international financial groups. The framework providing for cooperation with other EU supervisors is very broad and comprehensive. It is the following provisions:

- Section 25 par.2, Section 26c, Section 38h and Section 38ha of the Act on Banks
- Section 22a, Section 22aa, Section 22b, Section 25d, Section 25g, Section 25l of the Act on Credit Unions
- Section 26 of the Law on Supervision in the Capital Market (no. 15/1998 Coll.)
- Section 27, 135a and Section 152 and following of the Capital Market Undertakings Act
- Section 576 and following of the Act on Management Companies and Investment Funds

- Section 84 par.4, Section 92e, Section 92j, Section 133 of the Insurance Act
- Section 135b of the Law on Payment Institutions
- Section 140 and following of the Act on Consumer Credit

479. Information exchange with foreign counterparties is exempt from confidentiality *obligations (subject to the condition of similar confidentiality standard of the counterpart)*

- Section 25a of the Act on Banks
- Section 25a of the Act on Credit Unions
- Section 26 of the Law on Supervision in the Capital Market (no. 15/1998 Coll.)
- Section 128 par.3 of the Insurance Act
- Section 135b of the Law on Payment Institutions
- Section 17 par.4 of the Act on Bureau-de-change Activity
- Section 137 of the Act on Consumer Credit

480. Concerning non-EU counterparts, as referred in c. 40.12 CNB can cooperate and negotiate MoUs with other countries (MoUs normally include the exchange of information for AML/CFT supervisory purposes). At the same time for non EU countries without MoUs Czech legislation does not provide explicitly for the banking secrecy information exchange and it is not clear whether the general provision in the Act on the CNB is sufficient to enable the CNB to cooperate with non-EU counterparts without a concluded agreement.

481. *Criterion 40.14* – The scope of the information that the CNB is able to exchange (on the basis of legislation, in the manner, to the extent and within limitations described under c.40.13) is not restricted and can therefore include regulatory, prudential and AML/CFT information.

482. *Criterion 40.15* – The CNB is able to conduct inquiries and investigations on behalf of foreign counterparts and exchange with foreign counterparts all information obtained if such inquiries were being carried out domestically (see R40.12 - 40.13). The CNB may ask the supervisory authority of the relevant country for an on-site examination of the entities it supervises outside the territory of the CzR. The CNB may meet the request of the home country supervisory authority of a foreign bank or authorised financial institution for the carrying-out of an on-site examination of an entity it supervises. However, the CNB may not always be able to authorize or facilitate the ability of foreign counterparts to conduct inquiries themselves in CzR, in order to facilitate effective group supervision, especially if foreign counterparty is located in non-EU country and there is no cooperation agreement between supervisors concluded.

483. *Criterion 40.16* – The CNB Memoranda of understanding require parties not to disclose any confidential information to third parties without prior written consent of the party that has provided this confidential information. If the disclosure of confidential information to a government agency is required by the law, the party should promptly notify the party that has provided the confidential information.

Exchange of information between law enforcement authorities

484. *Criterion 40.17* – Police is able to exchange domestically available information with foreign counterparts. The rules of this cooperation are set up in the Title XI- International Cooperation of the Act on the Police of the CzR as well as in the Binding instruction No. 270/2013 on "Law enforcement procedures in certain areas of international cooperation in criminal matters". The latter allows a police officer to choose the most appropriate and effective tool when rendering an international

cooperation to foreign counterparts. Prosecutors can exchange information with their foreign counterparts to be used as intelligence or for investigations based on S.56 of the IJCCM.

485. The information regarding tracing and identifying proceeds and instrumentalities of crime is exchanged with counterparts from EU MS via Asset Recovery Offices (ARO) channel. The Czech Republic ARO executes tasks of the specialised central office under Council Decision 2007/845/JHA which sets cooperation Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime. The Czech ARO forms part the NOCA thus a binding instruction No 103/2013 on performance of tasks in the criminal proceedings (as issued by Police) also includes ARO' tasks: to act as a central office in relation to asset recovery matters within the Czech Police; to gather and to share best practice, support financial investigators in their efforts to trace and seize criminal assets and to supply them with information obtained from AROs of other Member States as well as to process and reply incoming requests from other AROs.

486. *Criterion 40.18* – According on the Section 91 of the Police Act, the Police may, upon request of the foreign counterparts, use supportive operative means or operative means of investigation in line with the CPC. Section 89 of the Police Act states that, when meeting their tasks, the Police shall cooperate with the International Criminal Police Organisation - Interpol, the European Police Office, relevant authorities and institutions of the European Union and its Member States, as well as with other international organisations, foreign security forces and other competent foreign entities. The Binding Instruction No. 78/2009 on the activities of NCB Prague regulates cooperation with Interpol and its members, while the Binding Instruction No. 183/2011 on Cooperation with Europol sets up rules of information exchange with and via the European Police Office. Prosecutors can ensure such cooperation through Eurojust.

487. *Criterion 40.19* – The law enforcement authorities of the CzR are able to form joint investigative teams as regulated by Sections 71-74 of the IJCCM. The competent authority for concluding such an agreement is the SPPO. Other arrangements to enable joint investigations are available under Europol and Eurojust frameworks.

Exchange of information between non-counterparts

488. *Criterion 40.20* – Some examples of exchange of information between non-counterparts have been provided by the Czech authorities. According to the AML/CFT Act, the FAU can exchange information with state bodies of foreign countries competent for the prevention and detection of money laundering and terrorism financing at their written and grounded request or on its own initiative. In practice, the FAU prefers exchange of information via foreign FIU.

489. FAU is able to exchange information with foreign non-FIU authorities (S.33 of the AML/CFT Act). The authorities advised that the FAU can deliver information to domestic authorities on request of foreign counterparts of these authorities (e.g. if police authority asks the FAU for information on behalf of foreign police authority) and that it can request information from the foreign FIU on behalf of other domestic authority. In case the FAU provides information to foreign FIU which needs to be forwarded to the third party, the prior written consent of the FAU is always required.

490. Although Section 89 of the Police Act foresees that the Police shall cooperate with Interpol, Europol, relevant authorities and institutions of the European Union and its Member States, as well as with other international organisations, foreign security forces and other competent foreign entities, it is not clear if it can exchange operational data with non-counterparts.

Weighting and Conclusion

491. **Czech Republic is Largely Compliant with R.40**

SUMMARY OF TECHNICAL COMPLIANCE – KEY DEFICIENCIES

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• There is no requirement for FIs and DNFBPs to take enhanced measures to manage and mitigate the higher risks identified in the NRA or to incorporate information on those risks into their risk assessments. • the lower risk situation identified by the AML/CFT Act is not fully supported by the NRA findings. • the legislation does not require DNFBPs to monitor the implementation of policies, controls and procedures and take enhanced measures to manage and mitigate the risks where higher risks are identified.
2. National cooperation and coordination	PC	• Structures which would include regularly scheduled contacts, linking the FAU as coordinator and the relevant agencies and private sector stakeholders, as opposed to sporadic or *ad hoc* contacts, are not in place. • there is an ambiguity about the formal designation and authorisation in law or regulation as to the agency or agencies responsible for the coordination of PF related issues.
3. Money laundering offence	LC	• The legislation does not clearly cover "possession". • whilst the self-laundering is covered by S. 216 of the CC, it does not extend to "participation" and "favouritism" (sections 214 and 366 of the CC).
4. Confiscation and provisional measures	C	
5. Terrorist financing offence	LC	• Funds or property "in full or in part" being destined for use by terrorists or in the commission of terrorist offences are not fully covered by the law but only by its interpretative note.
6. Targeted financial sanctions related to terrorism & TF	PC	• A formal mechanism for identifying and designating targets do not extend to UNSCR 1988. • no clear evidentiary standard and procedure apply to designation proposals, including upon foreign request. No provision ensures that a prompt determination can be made on a third party listing request. • freezing cannot apply to EU nationals at EU level (UNSCR 1373). • there are no clear provision to ensure that as much information as possible would be given to third countries in case a listing request is made. • targeted financial sanctions are not implemented without delay. • application of freezing is based on a discretionary decision, and applied mechanism does not ensure permanent application of measures, for the duration of validity of the UN actions. • the scope of funds to be frozen are ambiguous in national legislation, and do not extend to sufficiently broad range of assets. • de-listing and unfreezing procedures do not explicitly cover the delisting requirement under UNSCR 1988, and is not publicly available.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
7. Targeted financial sanctions related to proliferation	PC	• Deficiencies reflected under R.6 apply accordingly. • at national level there are no formal mechanisms in place for de-listing persons and entities and un-freezing funds. • there is a lack of guidance to the obliged entities on TFS.
8. Non-profit organisations	PC	• No subset of NPOs meeting the FATF definition or systematic identification of higher FT risk NPOs and related threats specific for the country are identified. • the periodicity of assessment of the sector is not defined. • there is no specific CFT outreach to NPOs and donors provided, no best practices developed, and no encouragement to use regulated financial channels take place. • no mechanisms of targeted risk-based supervision/monitoring of NPOs is in place.
9. Financial institution secrecy laws	C	
10. Customer due diligence	LC	• No explicit restriction to maintain anonymous accounts; • no specific reference to legal arrangements for the customer identification purposes; • there is no requirement that the verification of the identity of legal persons and legal arrangements should be based on reliable, independent sources and information; • definition of BO is incomplete does not include natural persons on whose behalf a transaction is being carried out; • no obligation to also understand the purpose and intended nature of the business relationship; • no specific provision for the keeping up-to-date and relevant collected CDD documents or for reviewing existing CDD records particularly for higher risk categories of customers; • not specifically required to understand the nature of the customer's business; • no specific requirement to obtain proof of existence of legal arrangements; • no specific requirements for the obliged entities to include the beneficiary of a life insurance policy as a relevant risk factor when determining whether to apply enhanced CDD measures; • no requirement to do this on the basis of materiality and risk nor to take into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained; • no explicit requirement for the obliged entities to perform EDD where the ML/FT risks are higher; • lower risk customer categories have not been identified through an adequate analysis of risks by the country or the financial institution; • no explicit provision enabling the obliged entities not to apply CDD if there is a risk of tipping-off the customer and report a STR.
11. Record keeping	LC	• No clear requirement for non-financial sector to maintain records on account files, business; correspondence and/or results of any relevant analysis; • no requirement to maintain transaction records in a manner enabling reconstruction of individual transactions to assist investigations.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
12. Politically exposed persons	LC	• The requirement of c. 12.4 does not extend to the beneficial owner of the beneficiary; there is no requirement to inform senior management when higher risks are identified, to conduct enhanced scrutiny on the whole business relationship or to consider making an STR.
13. Correspondent banking	PC	• There is no requirement to understand the AML/CFT responsibilities of the institutions engaged in the correspondent banking; • there is no explicit requirement covering EC 13.2 (a).
14. Money or value transfer services	C	
15. New technologies	LC	• The assessment of risks associated with new products, technologies and practices is not complete; • there is no specific requirement for the up-date the risk assessment prior to the launch or use of such technologies.
16. Wire transfers	LC	• Data on originator and beneficiary information is not fully compliant with R11; • the information on the beneficiary is not maintained fully in line with R11 requirements; • no specific requirement for a MVTS that controls both the ordering and the beneficiary side of a wire transfer.
17. Reliance on third parties	LC	• No specific requirement that the information should be obtained immediately, nor that copies and documentation are to be made available by the third party upon request and without delay; • legislation does not require analysis of ML/FT risks on third party's country of origin.
18. Internal controls and foreign branches and subsidiaries	LC	• No specific provision requiring screening of employees before hiring, to ensure high standards; • no requirement in the law regarding the provision at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries, when necessary; • no clear requirement to appoint a compliance officer at management level.
19. Higher-risk countries	PC	• No specific obligation to apply EDD for customers from high-risk countries; • insufficient counter-measures (19.2).
20. Reporting of suspicious transaction	PC	• The definition of STR does not cover criminal activities that would constitute a predicate offence for ML; • the reporting timeframe is not in line with the notion of "promptness".
21. Tipping-off and confidentiality	PC	• Insufficient provisions on protection of the directors, officers and employees of the REs from liability for the reporting of data in good faith to the FAU.
22. DNFBPs: Customer due diligence	PC	• Some independent legal professionals are not covered by the MAL.CFT obligations; • the law does not specify that the services also include preparing for or carrying out transactions concerning the activities in R.22; • insufficient definitions and obligations for TCSPs; • no clear requirement in the AML/CFT Law for DNFBPs to

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		maintain records on account files, business correspondence and/or results of any relevant analysis and it is not explicitly required to retain the records in a way suitable to reconstruct individual transactions; • deficiencies with respect to information that should be obtained immediately and documents available without delay.
23. DNFBPs: Other measures	PC	• Deficiencies identified under R18, R19, R20 and R21 apply; • lawyers, notaries and accountants are not obliged to have to have written system of internal rules, procedures and control measures.
24. Transparency and beneficial ownership of legal persons	LC	• The NRA does not assess the risks of all types of legal persons created in CzR; • associations are not obliged to maintain a list of its members; • not all legal persons are required to maintain information on their shareholders or members; • no requirement to verify the information about the beneficial owner; • no requirement for the legal person (or its administrators, liquidators or other persons involved in the dissolution of the company) to keep the information after its dissolution; • no mechanism to prevent nominee shareholders or managers; • no direct administrative or criminal liability for legal and/or natural person for incorrect data submission to the Register of Information on Beneficial Owners; • no formal mechanism to ensure the quality of the assistance received by the Czech authorities in response to requests for basic and BO information.
25. Transparency and beneficial ownership of legal arrangements	LC	• No specific responsibility for the trustees to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors; • the legislation does not specify records retention requirements for professional trustees; • the obligation for the trustees to disclose their status is indirect; • no sanctions for incorrect data submission to the BO Register by trustees.
26. Regulation and supervision of financial institutions	LC	• Exceptions in the application of fit and proper test by CNB; • the risk based approach in supervision by the CNB Financial Market Supervision Department II would benefit from being more AML/CFT driven; • FAU`s risk assessment systems partially correspond with requirements of 26.5(a) and 26.5(b) with no indication of 26.5(c); • no formal approved procedure or regulation of FAU or CNB for periodic review of the ML/FT risk profile of financial institution of groups and when there are major events or developments occur.
27. Powers of supervisors	LC	• There are no sanctions on suspending or restricting licenses.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
28. Regulation and supervision of DNFBPs	LC	• Real-estate agents not subject to authorization; • no requirement for these SRBs to apply risk-sensitive approaches to supervision; • supervision is not performed on a risk-sensitive basis for casinos, lawyers and notaries.
29. Financial intelligence units	LC	• The ability of the FAU to conduct strategic analysis is not explicitly covered and no strategic analysis product except from the NRA has been developed by the FAU. • the FAU powers are limited and do not cover dissemination of information to LEAs upon request.
30. Responsibilities of law enforcement and investigative authorities	LC	• CPC does not provide a clear definition of the financial investigation neither designates specific law enforcement authority to 'trace and identify' the proceeds of crime.
31. Powers of law enforcement and investigative authorities	C	
32. Cash couriers	PC	• The declaration system applies only to movements (both inward and outward) of cash and BNI from and to the EU. • there is no regulation that would require customs to stop or restrain currency of BNIs for a reasonable time in order to ascertain whether there is a suspicion that ML/FT or predicate offences were committed.
33. Statistics	PC	• ML statistics are not segregated by types of cases (stand-alone ML, self-laundering). The authorities do not keep accurate statistics on confiscation, MLAs or other international requests for cooperation received.
34. Guidance and feedback	LC	• There is no formal obligation for the authorities to provide guidelines to the obliged entities.
35. Sanctions	PC	• Not all the requirements of R 19 are such sanctionable; • the maximum level of sanctions is not dissuasive enough; • limited applicability of sanctions for natural persons.
36. International instruments	LC	• CzR ratified and brought into force the Palermo, Mérida and Terrorist Financing Conventions, whilst the evidence of their full implementation appears still to be lacking.
37. Mutual legal assistance	LC	• Minor deficiencies identified in relation to R. 3 and R. 5 can limit the scope of the assistance available because of the requirement of dual criminality for coercive measures; • complete and centralised case-management system is yet not in place.
38. Mutual legal assistance: freezing and confiscation	LC	• The recognition and execution of foreign NCB (non-conviction based) forfeiture can only be done when the requesting state has a similar concept of NCB forfeiture in criminal proceedings.
39. Extradition	LC	• When refusal of surrender is based solely on nationality, it is possible for CzR authorities to take the matter before a CzR court. However there does not seem to be an obligation to do so at the request of the foreign state.
40. Other forms of international cooperation	LC	• Apart from the FAU, there are no specific legal provisions for other authorities regulating explicitly the provision of feedback to the authority from which assistance was sought and

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		providing this in a timely manner. • it is not clear whether the general provision in the Act on the CNB is sufficient to enable the CNB to cooperate with non-EU counterparts without a concluded agreement. • it is not clear from the legislation if the police can exchange operational data with non-counterparts.

GLOSSARY OF ACRONYMS

AML/CFT Act	Act on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism
AMO	Asset Management Office
BNI	Bearer negotiable instrument
BO	Beneficial Ownership
CARIN	Camden Asset Recovery Interagency Network
CC	Criminal Code
CDD	Customer due diligence
CFT	Countering the financing of terrorism
CNB	Czech National Bank
CPC	Code of Criminal Procedure
CPF	Countering PF
CZK	Czech koruna (Czech currency)
CzR	Czech Republic
DNFBP	Designated non-financial business and profession
DPMS	Dealers in precious metals and stones
DPRK	Democratic People's Republic of Korea
EDD	Enhanced Due Diligence
EU	European Union
EUR	euro
FATF	Financial Action Task Force
FAU	Financial Analytical Unit (Czech FIU)
FI	Financial institution
FIU	Financial Intelligence Unit
FinCEN	US Financial Crimes Enforcement Network
FTF	Foreign terrorist fighter
FT	Financing of terrorism
RVNNO	Government Council for Non-Governmental Non-Profit Organizations
IAIS	International Association of Insurance Supervisors
IIS	Act on Implementation of International Sanctions
Interpol	International Criminal Police Organisation
IOIWG	Inter-institutional Open Informal Working Group
ISAs	International Standards on Auditing
IJCCM	Act on Judicial Cooperation in Criminal Matters
IO.	Immediate outcome
IOSCO	International Organisation of Securities Commissions
ISIL	So called 'Islamic State of Iraq and the Levant'
IT	Information technology
JITs	Joint investigation teams
LEA	Law enforcement authority
MER	Mutual evaluation report
MI	Methodological Instruction
ML	Money laundering
MLA	Mutual legal assistance
MoU	Memorandum of understanding
MVTS	Money or value transfer service

MEQ	Mutual evaluation questionnaire
NCBC	Non-conviction based confiscation
NCPT	National Contact Point against Terrorism
NOCA	National Organised Crime Agency of the Police
NPO	Non-profit organisation
NRA	National risk assessment
NSA	National Security Audit
OGRPA	Office of the Government Representation in Property Affairs
Palermo Convention	UN Convention Against Transnational Organised Crime
PEP	Politically exposed person
PF	Financing of proliferation of weapons of mass destruction
PPO	Public Prosecutor's Office
R.	Recommendation
S.	Section/article of the legal act
SRBs	Self-regulatory bodies
STR	Suspicious transaction report
SR.	Special Recommendation
TC	Technical compliance
TF Convention	International Convention for Suppression of the Financing of Terrorism
TFS	Targeted financial sanctions
UCCFC	Unit Combating Corruption and Financial Crime
UN	United Nations
UNCAC (also known as Merida Convention)	UN Convention against Corruption
UNSC	UN Security Council
UNSCR	UN Security Council Resolution
US	United States
USD	US dollars
VAT	Value added tax
Vienna Convention	UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
WCO	World Customs Organisation

www.coe.int/MONEYVAL

December 2018

Anti-money laundering and counter-terrorism financing measures

Czech Republic

Fifth Round Mutual Evaluation Report

This report provides a summary of AML/CFT measures in place in Czech Republic as at the date of the on-site visit (5 to 16 March 2018). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Czech Republic's AML/CFT system, and provides recommendations on how the system could be strengthened.