COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Project on "Countering Economic Crime in Serbia"

TECHNICAL PAPER

Business and Technical Requirements for upgrade of the Centralised Anti-Money Laundering Database

ECCD-CECS-SRB-TP1-2026 Date: 02/2026

The project **"Countering Economic Crime in Serbia"** aims to strengthen Serbia's institutional capacity to combat money laundering and related economic crime by supporting the development of comprehensive business and technical requirements for the upgrade of the Centralised Anti-Money Laundering Database (CAML) used by the Supreme Public Prosecutor's Office (SPPO) and other relevant authorities. Within this framework, an assessment mission will analyse the current system architecture, user needs, data quality mechanisms, interoperability, security, and reporting functionalities, and define clear specifications for enhanced case tracking, monitoring, and compliance features. The activity is implemented under the Council of Europe, ensuring that the upgraded CAML system will provide improved usability, data reliability, and operational effectiveness in Serbia's anti-money laundering framework.

The project is funded by Sweden, represented by the Swedish International Development Cooperation Agency and implemented by the Council of Europe.

TABLE OF CONTENTS

ABBREVIATIONS

API	Application Programming Interface
CAML	Centralised Anti-Money Laundering Database
COE	Council of Europe
HTTPS	Hypertext transfer protocol secure
JSON	JavaScript Object Notation
SPPO	Supreme Public Prosecutor's Office
REST	Representational State Transfer
SOAP	Simple Object Access Protocol

1 EXECUTIVE SUMMARY

The project "Countering Economic Crime in Serbia" aims to strengthen Serbia's institutional capacity to combat money laundering (ML) and terrorist financing (TF) through the development of comprehensive business and technical requirements for the upgrade of the Centralised Anti-Money Laundering Database (CAML). CAML currently functions as a national case registration and statistical monitoring platform used by 21 competent authorities, including prosecution offices, courts, law enforcement bodies and financial oversight institutions. While technically stable and security-focused, the system was originally designed primarily as a structured registry and statistical tool. The assessment mission identified operational limitations in advanced analytics, cross-institution performance monitoring, automated data validation, interoperability with external databases, and real-time monitoring capabilities.

The proposed upgrade will transform CAML into an integrated national AML/CFT monitoring, analytical and coordination platform. The upgraded system will support full lifecycle case tracking across institutions, introduce real-time dashboards and alert mechanisms, enhance data quality controls, enable structured interoperability where legally and technically feasible, and align reporting outputs with evolving international standards (MONEYVAL, FATF, EU and World Bank methodologies). The solution will preserve strict institutional data isolation and high-level security architecture while significantly expanding analytical functionality, usability and strategic reporting capacity.

By strengthening data reliability, operational transparency and cross-institution coordination, the project will enhance Serbia's ability to monitor AML/CFT performance, identify systemic bottlenecks, conduct national risk assessments and meet international evaluation requirements. The upgrade of CAML will therefore serve not only as a technical improvement, but as a structural reinforcement of Serbia's overall framework for countering economic crime. The upgrade is conceived as an institutional enhancement of the existing CAML system, with full ownership and administrative control to remain within the national prosecution framework.

2 DESCRIPTION OF THE CURRENT SITUATION AND IMPACT OF THE DIGITAL SERVICES PROJECT

The existing Centralised Anti-Money Laundering Database (CAML) represents a technically stable and security-oriented case management platform that has been operational since 2011 and upgraded most recently in 2023–2024. The system operates through 21 logically and technically separated institutional instances, ensuring strict data isolation between competent authorities involved in the AML/CFT chain. It supports structured registration of money laundering (ML) and terrorist financing (TF) cases, persons, criminal offences, assets, procedural actions, judicial outcomes, and international cooperation. The current architecture—based on Ubuntu Server, Apache, PHP, MySQL and Apache Solr—provides solid performance, audit logging, two-factor authentication and controlled inter-instance data exchange via push-based web services. However, the assessment identified several structural and operational limitations, including incomplete historical data entry, lack of automated interoperability with external state databases, limited cross-instance analytical aggregation, absence of real-time dashboards and alert mechanisms, and evolving international reporting requirements that exceed the system's original statistical tracking design.

The Digital Services Project will directly address these gaps by transforming CAML from a primarily case registration and statistical reporting tool into an integrated national AML/CFT monitoring and analytical platform. The upgrade will introduce end-to-end lifecycle case tracking, real-time dashboards, automated time-in-procedure monitoring, structured alert mechanisms, enhanced data validation controls, advanced analytical and strategic reporting, and configurable international reporting outputs aligned with MONEYVAL, FATF and EU standards. Furthermore, conditional API-based interoperability with the Ministry of Interior and Tax Administration databases will reduce manual data entry, improve data reliability and enable controlled data standardisation across institutions. By preserving the existing principles of institutional isolation and high-level security while significantly expanding analytical capacity, interoperability and usability, the project will strengthen evidence-based decision-making, improve operational efficiency, enhance national risk assessment capabilities, and increase Serbia's overall institutional resilience in combating economic crime and money laundering.

3 DESCRIPTION OF THE EXISTING SYSTEM

The Centralised Anti-Money Laundering Database (CAML) is a national case management and statistical monitoring platform designed to support the tracking of money laundering (ML) and terrorist financing (TF) cases across multiple Serbian state authorities. The system was originally developed under EU and subsequent international support projects and has been operational since 2011, with significant upgrades completed in 2023–2024.

CAML serves as a collaborative yet technically decentralised platform used by 21 competent authorities involved in the AML/CFT chain. Its primary objective is to ensure comprehensive case registration, enable structured statistical reporting, and provide traceability of cases from initial detection through prosecution, adjudication and asset confiscation. The system supports the full procedural lifecycle of ML and TF cases and enables structured collection of data necessary for national and international reporting obligations.

Although referred to as a "centralised" database, the system is architecturally implemented as a federation of isolated institutional instances hosted within a common infrastructure environment.

3.1 Institutional Coverage and Operational Model

The system currently operates through 21 separate instances, each dedicated to a specific institution or organisational unit. These include:

- Supreme Public Prosecutor's Office (SPPO)
- Public Prosecutor's Office for Organised Crime
- Specialised anti-corruption prosecution offices
- Higher courts (including specialised departments)
- Financial Intelligence Unit (USPN)
- Ministry of Interior (MUP units including SBPOK and JFI)
- Tax Administration
- Customs Administration
- Ministry of Justice – International Legal Assistance Department
- Directorate for Management of Seized Assets
- Security Information Agency (BIA)

Each institution operates within its own logically and technically isolated instance of the system. Data entered in one instance is not directly visible to other institutions. Information sharing between institutions is possible only through explicitly initiated structured electronic acts using a controlled "push" web service mechanism .

This architecture ensures institutional data autonomy and minimises risks of unauthorised access. Even in the hypothetical case of credential compromise, access would be limited strictly to the compromised institutional instance.

3.2 Functional Scope of the Existing System

CAML is a web-based case management system that enables structured registration and monitoring of:

- ML and TF cases
- Physical and legal persons involved in proceedings
- Criminal offences (ML, TF and predicate offences)
- Assets linked to cases
- Procedural actions and decisions
- International cooperation and legal assistance
- Suspicious transaction reports
- Judicial outcomes and sanctions

The system supports horizontal and vertical tracking of case chains. It enables linking of cases between institutions, allowing construction of procedural chains from initial suspicion (e.g. Police, FIU or Customs) through prosecution and court decisions, up to asset management and confiscation.

The core functional modules include:

1. **Case Registration Module** – Structured registration of ML and TF cases with procedural metadata, initiator information and institutional references.
2. **Persons Module** – Registration of natural and legal persons with detailed identifiers (JMBG for individuals, PIB/MB for legal entities), roles in proceedings, and AML typology classification.
3. **Criminal Offences Module** – Structured classification of offences under relevant laws, including predicate offences and sector-specific typologies.
4. **Asset Tracking Module** – Registration, categorisation and valuation of movable and immovable assets, including status changes (freeze, seizure, confiscation).
5. **Procedural Actions Module** – Logging of all institutional actions with timestamps, recipients and links to related acts.
6. **International Cooperation Modules** – Separate modules for international legal assistance and international cooperation.
7. **Judicial Decision Module** – Recording of first- and second-instance court decisions, sanctions and outcomes.
8. **Reporting Module** – Generation of statistical reports and case summaries.
9. **Audit Log Module** – Immutable logging of all user actions and data changes.
10. **Codebook Administration Module** – Centralised management of controlled vocabularies (by SPPO instance).
11. **User Management Module** – Instance-level user administration and role assignment.

3.3 Technical Architecture

The CAML system is deployed within the data centre of the Supreme Public Prosecutor's Office. It operates in a virtualised environment using VMware infrastructure.

3.3.1 Server Environment

The server-side environment consists of:

- Ubuntu Server 24.04 LTS
- Apache HTTP Server
- PHP 8.3
- MySQL relational database
- Apache Solr enterprise search platform

The system is dimensioned for hundreds of concurrent users and tens of thousands of cases.

3.3.2 Database Architecture

The data storage architecture is hybrid:

- **MySQL** is used for relational storage of metadata, user accounts, codebooks, audit logs and transactional control.
- **Apache Solr** is used as the primary storage and indexing engine for case content, enabling high-performance full-text search and near real-time indexing.

This separation allows rapid querying and complex filtering, particularly for analytical and statistical purposes. Solr provides scalability and resilience by design and supports horizontal scaling.

3.3.3 Instance Separation

Each of the 21 institutions operates a fully separated instance with:

- Separate database schema
- Separate application configuration
- Separate subdomain
- Isolated data visibility

Inter-instance communication is possible exclusively via controlled web service exchange of structured acts.

3.4 Network Architecture and Access Control

The system is accessible exclusively through:

- Judicial network
- State administration network

- VPN connection (FortiClient) to the judicial network

Direct access from the public internet is not possible.

All communication between client and server is conducted over HTTPS. The system is fully browser-based and requires no local software installation.

3.5 Authentication and Authorisation Model

CAML uses multi-factor authentication (2FA) based on:

- Username and password
- Time-based one-time token generated by Google Authenticator

User manual for CAML v1.0

Role-based access control is implemented at instance level. Roles include:

- Super Administrator
- Administrator
- Super-user (SPPO analytical role)
- Data-entry officer
- Head of institution

Each role determines visibility and modification rights.

All user actions are recorded in an immutable audit log, including login attempts, data modifications, and IP address of access.

3.6 Data Management and Backup Policy

The system employs daily automated backups using Amanda Open Source Backup system. Full backups are performed daily during off-peak hours and retained for 30 days.

Audit logging is systematic and cannot be bypassed. No data modification can occur without being recorded in the historical log.

3.7 Current Operational Challenges Identified During Assessment

Despite its robust architecture and structured data model, several operational and structural limitations exist:

1. Data-entry inconsistencies and incomplete historical records (not all cases from 2012 onward entered).
2. Lack of automated integration with external systems (MUP Oracle database, Tax Administration valuation database).
3. Absence of real-time analytical dashboards and alert mechanisms.

4. Limited ability to perform cross-instance analytical aggregation at national level.
5. Missing classification elements (e.g., types of international legal assistance, direction of decisions).
6. Manual parallel record-keeping in some institutions (Excel and paper-based records in MUP).
7. Evolving reporting standards (EU, MONEYVAL, FATF) requiring expanded datasets.
8. Usability challenges in data-entry processes.
9. Session timeout configuration causing operational friction.
10. No structured automated data quality validation module.

3.8 Summary of the Current System State

The existing CAML system is a technically stable, security-focused and modular AML/CFT case management platform. It provides strong institutional data isolation, structured classification of AML/TF cases, detailed asset tracking and comprehensive audit capabilities.

However, it was originally designed primarily as a statistical tracking and case registration tool. Its current architecture and functional model require enhancement to meet modern requirements for:

- Advanced analytics and risk assessment,
- Cross-institution performance monitoring,
- Automated data validation,
- Real-time monitoring,
- API-based interoperability,
- Expanded international reporting obligations.

The upgrade therefore builds upon a solid technical foundation but must address functional expansion, interoperability, usability improvements and enhanced analytical capabilities.

3.9 Budget of the project

The project's budget is capped at 160000 EUR, allocated for all of the project stages including initial planning, development and testing environments setup, application development, production environment installation, configuration, training, and project management.

4 BUSINESS REQUIREMENTS FOR THE UPGRADE

4.1 General Objective of the Upgrade

The upgrade of the Centralised Anti-Money Laundering Database (CAML) shall transform the system from a primarily structured statistical registry into an integrated national AML/CFT monitoring, analytical and coordination platform.

The upgraded system shall:

- Support full lifecycle monitoring of AML and TF cases across institutions.
- Improve data completeness, consistency and reliability.
- Enable real-time operational monitoring.
- Provide advanced analytical and strategic reporting tools.
- Support evolving international AML/CFT reporting standards (EU, MONEYVAL, FATF, World Bank).
- Facilitate controlled interoperability with external state databases.
- Improve usability and reduce administrative burden on data-entry staff.

The business requirements below reflect findings from the assessment mission conducted with the SPPO, Ministry of Justice, MUP, Tax Administration and other stakeholders.

4.2 Case Lifecycle Monitoring and Tracking

4.2.1 End-to-End Case Chain Tracking

The upgraded system shall enable visual and analytical tracking of the complete lifecycle of AML/TF cases across institutions, from:

- Initial suspicion (FIU, MUP, Customs, Tax Administration),
- Prosecutorial proceedings,
- Court adjudication,
- Asset seizure and confiscation,
- Final asset disposition.

The system shall automatically construct and display case chains across institutions based on linked case numbers and exchanged acts, enabling SPPO and authorised analytical users to see:

- Origin of case,
- Current status,
- Procedural stage,
- Institutions involved,
- Duration of each stage.

4.2.2 Real-Time Case Status Monitoring

The system shall provide real-time dashboards displaying:

- Number of active AML cases,
- Number of TF cases,
- Cases per procedural stage,
- Cases with seized/confiscated assets,
- Cases exceeding predefined procedural time thresholds.

The system shall allow filtering by:

- Institution,
- Year,
- Type of offence,
- Sector typology,
- Asset category,
- Geographic area.

4.2.3 Time-in-Procedure Monitoring

The upgraded CAML shall automatically calculate and display:

- Time elapsed since case opening,
- Duration of prosecutorial phase,
- Duration of judicial phase,
- Time between seizure and confiscation,
- Time to final resolution.

The system shall generate alerts for cases exceeding predefined time thresholds configurable by administrators.

4.3 Advanced Analytical and Strategic Reporting

4.3.1 Operational Statistical Reporting

The system shall support automated generation of:

- Monthly, quarterly and annual AML/TF statistics,
- Number of cases per offence type,
- Number of persons prosecuted,
- Conviction rates,

- Average sentence lengths,
- Number and value of seized/confiscated assets,
- Ratio of seized to confiscated assets.

Reports shall be exportable in structured formats (Excel, CSV, PDF, machine-readable XML/JSON).

4.3.2 Strategic Risk Analysis

The upgraded system shall enable:

- Sector-based analysis (e.g., real estate risk assessment),
- Geographic risk mapping,
- Typology trend analysis,
- Identification of frequently recurring persons,
- Identification of systemic bottlenecks in case progression.

The system shall support annual national AML risk analysis reporting and enable extraction of datasets compliant with international standards.

4.3.3 International Reporting Compliance

The system shall support structured data extraction aligned with:

- MONEYVAL statistical templates,
- FATF Immediate Outcome indicators,
- EU AML reporting standards,
- World Bank performance metrics.

The system shall allow configurable reporting fields to adapt to evolving international methodologies.

4.4 Data Integration and Interoperability

The data integration and interoperability components of the upgrade shall be implemented only to the extent that the respective external institutions (e.g., MUP, Tax Administration and other relevant authorities) possess the legal, technical and organisational capacity to support secure direct system-to-system integration with their existing solutions.

4.4.1 Integration with MUP Criminal Database

The system shall enable controlled integration with the MUP Oracle-based criminal records database for:

- Automatic retrieval of general person data,
- Verification of JMBG and identity data,
- Retrieval of basic case reference information.

Integration shall be implemented via secure APIs, subject to legal feasibility.

4.4.2 Integration with Tax Administration Property Database

The system shall enable integration with the Tax Administration valuation database in order to:

- Retrieve official real estate valuation data,
- Reduce manual entry errors,
- Ensure consistent asset valuation,
- Support real estate risk assessment.

4.4.3 Controlled Data Exchange Between Institutions

The existing push-based model shall be enhanced to:

- Allow structured partial data sharing,
- Support status synchronization where legally permitted,
- Provide confirmation receipts of exchanged acts,
- Allow tracking of response delays.

4.4.4 Data Standardisation Across Institutions

The upgrade shall ensure:

- Unified data taxonomy,
- Harmonised classification standards,
- Standardised terminology for international cooperation types,
- Direction tagging for decisions (incoming/outgoing),
- Structured categorisation of legal assistance types (minimum 10 categories).

4.5 Data Quality and Completeness Enhancement

4.5.1 Mandatory Data Enforcement

The system shall enforce mandatory entry of:

- JMBG for natural persons (or structured alternative ID for foreign nationals),
- PIB/MB for legal entities,
- Asset valuation where available,
- Procedural stage updates,
- International cooperation outcomes.

4.5.2 Logical and Chronological Validation

The system shall prevent:

- Entry of actions dated before case creation,
- Invalid status transitions,
- Duplicate persons within same instance,
- Logical inconsistencies in asset lifecycle.

4.5.3 Data Quality Dashboard

The system shall include an administrative dashboard indicating:

- Incomplete cases,
- Missing mandatory fields,
- Unvalued assets,
- Cases lacking outcome registration,
- Cases pending update beyond predefined period.

4.6 Asset Management Enhancement

The upgraded system shall:

- Track full asset lifecycle (freeze, seizure, temporary confiscation, permanent confiscation, destruction, return),
- Distinguish between temporary and permanent measures,
- Record post-confiscation disposition status,
- Allow linking of asset valuation updates,
- Support aggregation of total asset value per case and nationally,
- Allow export of asset statistics by category and year.

4.7 International Legal Assistance and Cooperation Upgrade

The system shall:

- Introduce structured categorisation of types of legal assistance (minimum 10 categories),
- Distinguish clearly between incoming and outgoing requests,
- Track response times,
- Record outcomes,
- Support statistical analysis by country and request type,
- Enable export of European standardised cooperation datasets.

4.8 Alert and Early Warning Mechanisms

The upgraded CAML shall include configurable alert mechanisms for:

- Frequently recurring persons across cases,
- Parallel investigations,
- High-value asset cases,
- Cases with no procedural update beyond defined period,
- Repeated appearance of same legal entity across institutions.

Alerts shall be visible only to authorised roles.

4.9 User Experience and Operational Efficiency

The system shall improve usability by:

- Simplifying data-entry forms,
- Reducing unnecessary duplication of input,
- Allowing auto-fill from integrated databases,
- Improving search filters and advanced search functions,
- Optimising 2FA login flow without reducing security,
- Allowing configurable session timeout within security limits.

4.10 Backlog Data Completion Support

Given the requirement to ensure that all cases from 2012 onward are entered into CAML, the upgraded system shall provide:

- Bulk import tools,
- Data validation tools for legacy entries,
- Monitoring dashboard for backlog completion,
- Reporting of institutional compliance with data entry obligations.

4.11 Performance and Scalability Requirements (Business Perspective)

From a functional perspective, the system shall:

- Support minimum 500 concurrent users,
- Maintain average query response time under 2 seconds,
- Allow horizontal scalability,
- Ensure no data loss during migration or upgrade,
- Maintain uninterrupted availability during critical operational periods.

4.12 Data Protection and Legal Compliance Requirements

Given the highly sensitive nature of data processed within the CAML system — including personal data of suspects, defendants, witnesses, asset holders and related persons — the upgraded system shall be fully aligned with applicable data protection legislation.

The solution shall ensure compliance with:

- The General Data Protection Regulation (GDPR) principles, where applicable,
- The Law on Personal Data Protection of the Republic of Serbia,
- Relevant criminal procedure and sector-specific legislation governing processing of data by law enforcement and judicial authorities,
- Applicable Council of Europe data protection standards.

The upgraded CAML system shall support the following data protection principles:

- **Lawfulness, Purpose Limitation and Legal Basis**

The system shall ensure that personal data are processed strictly within legally defined mandates of beneficiary institutions and solely for AML/CFT-related purposes.

Data Minimisation

The system shall collect and process only data that are necessary and proportionate for case management and statutory reporting.

Accuracy and Data Quality

The upgrade shall introduce validation mechanisms to prevent inaccurate or inconsistent personal data entries.

Storage Limitation

The system architecture shall support legally defined data retention periods and controlled archival mechanisms where required by law.

Integrity and Confidentiality

The system shall maintain high-level technical and organisational security measures, including:

- Role-based access control,
- Multi-factor authentication,
- Strict institutional instance isolation,
- Full audit logging,
- Encrypted communication (HTTPS),
- Controlled inter-instance data exchange.

Accountability and Auditability

The system shall maintain immutable audit logs enabling traceability of all access, modification and export of personal data.

Data Subject Rights (Where Applicable)

Where legally required and applicable, the system shall technically support the implementation of data subject rights, including:

- Access to data,
- Rectification,
- Restriction of processing,
- Logging of disclosures.

Implementation of such rights shall be subject to limitations applicable to criminal proceedings and law enforcement processing.

4.13 Summary of Business Transformation

The upgrade shall reposition CAML as:

- A national AML/CFT performance monitoring platform,
- A strategic analytical tool,
- A coordinated inter-institutional case tracking environment,
- A reliable statistical backbone for international evaluation,
- A data-driven decision-support system for policy makers.

The upgraded system must maintain existing security and institutional isolation principles while significantly enhancing analytical capacity, interoperability and operational effectiveness.

4.14 User Interface & Usability Requirements

The upgraded CAML system shall remain fully web-based and accessible through standard user workstations without requiring installation of any additional client-side software. The system shall be fully compatible with the latest stable versions of **Microsoft Edge** and **Google Chrome**, ensuring consistent functionality, performance, and security across both browsers. All user interface components, data-entry forms, reporting tools, dashboards, and authentication mechanisms (including 2FA) shall be tested and optimised for these browsers. The solution shall not rely on deprecated technologies or browser-specific plugins and must ensure responsive performance, secure HTTPS communication, and full feature availability within Microsoft Edge and Google Chrome environments used across participating institutions.

The upgraded system shall provide:

- Modernized responsive UI
- Simplified data-entry forms
- Contextual help
- Improved search filters

- Advanced search by:
  - Person
  - Asset
  - Institution
  - Case chain
- Reduced login friction while preserving 2FA
- Session timeout configuration improvements

5 IMPLEMENTATION OF THE SOLUTION

This section defines the framework for implementation of the upgraded CAML system, including project organisation, execution phases, testing and acceptance procedures, intellectual property rights, training activities, warranty support, and the overall implementation timeline. The provisions below shall be binding for the Provider selected through the procurement procedure.

5.1 Project Implementation Approach

The implementation of the upgraded CAML solution shall follow a structured, phased methodology ensuring controlled delivery, minimisation of operational risk, and full alignment with business requirements defined in this Technical Specification.

The Provider shall implement the solution through clearly defined stages including:

1. Project initiation and planning
2. Detailed functional and technical design
3. Development and configuration
4. Integration (where feasible and legally permitted)
5. Data migration (if applicable)
6. System testing
7. User acceptance testing (UAT)
8. Deployment to production environment
9. Training of users
10. Post-deployment warranty support

The Provider shall ensure that implementation does not disrupt ongoing institutional operations and that the production system remains stable throughout the transition period.

5.2 Project Organisation and Governance

5.2.1 Project Governance Structure

The project shall be implemented under a governance framework consisting of:

- Contracting Authority (Council of Europe / ECCD Secretariat)
- Beneficiary institutions (SPPO and other CAML users)
- Project Steering Group (if established)
- Provider's Project Team

The Provider shall appoint a Project Manager responsible for:

- Overall coordination of activities,

- Communication with the Contracting Authority and beneficiaries,
- Timeline management,
- Risk management,
- Quality assurance.

Regular coordination meetings (remote or in-person) shall be organised at agreed intervals.

5.3 Project Documentation

The Provider shall produce and maintain at minimum:

- Project Implementation Plan,
- Functional Design Document,
- Technical Architecture Document,
- Integration Design (where applicable),
- Testing Plan,
- Deployment Plan,
- Training Plan,
- Maintenance and Support Plan,
- Final Implementation Report.

All documentation shall be delivered in editable electronic format and in English (unless otherwise agreed).

5.4 Project Activities

The implementation shall include, but not be limited to, the following activities:

5.4.1 Analysis and Detailed Design

- Validation of business requirements with beneficiaries;
- Gap analysis between current system and target architecture;
- Definition of updated data models;
- Specification of reporting structures;
- Definition of interoperability interfaces (where feasible);
- Confirmation of security architecture,
- Validation of compliance data protection legislation and incorporation of privacy-by-design principles into the upgraded architecture.

No development shall begin before approval of the Detailed Design Documentation.

5.4.2 Development and Configuration

The Provider shall:

- Develop all required functional enhancements;
- Modify existing modules where necessary;
- Implement dashboards and analytics;
- Configure validation mechanisms;
- Develop integration interfaces (subject to institutional capability);
- Ensure backward compatibility with existing architecture unless justified alternative is approved.

Development activities shall be structured in two delivery waves:

- core system upgrade functionalities to be completed by 30 June 2026 (Phase 1); and
- advanced analytical and reporting modules to be completed by 31 December 2026 (Phase 2).

5.4.3 Data Migration and Backlog Support

If required, the Provider shall:

- Develop tools for bulk data import;
- Support cleansing and validation of legacy data;
- Ensure that no data loss occurs;
- Provide validation reports confirming migration integrity.

5.4.4 Integration Implementation (Conditional)

Integration components shall be implemented only if relevant institutions confirm their legal and technical capacity to support secure system-to-system integration.

The Provider shall:

- Develop secure APIs;
- Ensure encrypted communication;
- Provide integration testing documentation;
- Coordinate technical alignment with external system owners.

5.5 Testing and Acceptance of the Solution

Acceptance of Phase 1 (Core Upgrade) shall be formally documented no later than 30 June 2026.

Acceptance of Phase 2 (Advanced Reporting Modules) shall be formally documented no later than 31 December 2026.

5.5.1 Testing Phases

Testing shall be conducted in the following structured phases:

1. **Unit Testing** – Performed by the Provider.
2. **System Integration Testing** – Verification of module interoperability.
3. **Security Testing** – Including vulnerability assessment.
4. **Performance Testing** – Verification of response times and concurrent user load.
5. **User Acceptance Testing (UAT)** – Conducted with beneficiary representatives.
6. **Data Protection Compliance Verification** – Validation that implemented functionalities support applicable data protection requirements and privacy-by-design principles.

The Provider shall prepare a detailed Testing Plan including:

- Test scenarios,
- Acceptance criteria,
- Defect reporting procedures,
- Retesting procedures.

5.5.2 Acceptance Criteria

The system shall be considered accepted only if:

- All mandatory requirements are implemented,
- All critical and major defects are resolved,
- Performance benchmarks are met,
- Security requirements are satisfied,
- UAT sign-off is obtained from authorised beneficiary representatives,
- Where an independent security audit has been commissioned, all critical and high-risk findings have been resolved and formally validated..

Formal acceptance shall be documented in a signed Acceptance Report.

5.5.3 Independent Security Audit (Recommended)

In addition to the internal security testing performed by the Provider (including vulnerability assessment and security testing), the Contracting Authority and/or beneficiary institutions

may decide to commission an independent external security audit of the upgraded CAML system prior to final acceptance.

The purpose of such an audit shall be to:

- Assess the overall security posture of the upgraded system;
- Perform penetration testing and advanced vulnerability assessment;
- Verify compliance with industry security best practices;
- Validate the robustness of authentication, authorisation, session management, and access control mechanisms;
- Assess API security (where interoperability components are implemented);
- Review configuration of infrastructure and deployment environment.

If an independent security audit is conducted:

- The Provider shall grant the auditors reasonable technical access necessary for testing;
- Identified critical and high-risk vulnerabilities shall be remediated prior to final system acceptance;
- Remediation timelines for medium and low-risk findings shall be agreed with the Contracting Authority;
- A formal Security Audit Report shall be submitted and annexed to the Final Acceptance Report.

The independent security audit, if commissioned, shall be completed prior to formal Final Acceptance of the system.

5.6 Deployment

Deployment shall include:

- Installation in production environment,
- Configuration of infrastructure,
- Migration (if applicable),
- Go-live readiness check,
- Final security configuration,
- Backup verification.

Deployment shall be scheduled in coordination with SPPO IT staff to avoid operational disruption.

5.7 User Training

5.7.1 Training Scope

The Provider shall deliver structured training covering:

- New functionalities,
- Analytical dashboards,
- Reporting tools,
- Data validation mechanisms,
- Administrative functions.

Training shall be tailored to user categories including:

- Data-entry users,
- Prosecutors,
- Analytical staff,
- Administrators,

Super administrators. As part of Phase 1 (Core System Upgrade), the Provider shall deliver four (4) basic data-entry training sessions for end users of the CAML system.

These trainings shall focus specifically on:

- accurate data entry procedures,
- mandatory data validation requirements,
- case lifecycle registration,
- asset entry and status tracking,
- use of updated dashboards,
- correct classification of offences and typologies,
- proper recording of procedural actions and international cooperation data.

The objective of these trainings is to ensure uniform data quality standards and correct use of upgraded functionalities across all participating institutions.

5.7.2 Training Format

Training shall include:

- On-site sessions (minimum number as defined in Business Requirements),
- Remote sessions where appropriate,
- Practical demonstrations,
- Hands-on exercises.

Training materials shall include:

- Updated user manuals,
- Quick reference guides,
- Presentation slides,

- Optional video materials.

All materials shall be delivered in electronic format.

The four (4) basic data-entry trainings shall be delivered as in-person sessions in the following locations:

- Belgrade
- Kraljevo
- Niš
- Novi Sad

Each session shall be organised as a full-day training and shall include:

- practical demonstrations,
- hands-on exercises,
- real-case simulation scenarios,
- question-and-answer sessions.

The Provider shall prepare standardised training materials to ensure consistency across all locations.

5.8 Warranty and Support Period

The Provider shall provide warranty support for a minimum period of 12 months following final acceptance.

During the warranty period, the Provider shall provide:

- Corrective maintenance (bug fixing),
- Security updates,
- Minor configuration adjustments,
- Remote technical support,
- Incident resolution based on severity levels.

5.8.1 Service Levels

The Provider shall define response and resolution times based on incident severity categories (e.g., critical, major, minor).

Monthly support reports shall be submitted during the warranty period.

5.8.2 Copyright and Rights of Exploitation

All software components, source code, documentation, configurations, databases, design documentation and related materials developed under this contract shall become the exclusive property of the Supreme Public Prosecutor's Office (SPPO) of the Republic of Serbia, acting on behalf of all beneficiary institutions using the CAML system.

Given that the upgrade represents an enhancement and further development of an existing software solution and not the creation of a new proprietary product, the intellectual property rights over the upgraded solution shall remain within the institutional AML/CFT framework of the Republic of Serbia.

The SPPO shall have unlimited rights to:

- Use, modify and further develop the system;
- Maintain and administer the system independently or through third parties;
- Grant usage rights to all authorised institutional users of CAML;
- Ensure long-term sustainability and continuity of the system.

The Provider shall not retain ownership rights, proprietary claims, or usage restrictions over the upgraded system, except for explicitly declared third-party components licensed under their respective open-source or commercial licences.

5.9 Risk Management

The Provider shall:

- Identify implementation risks,
- Propose mitigation strategies,
- Maintain a Risk Register,
- Immediately notify the Contracting Authority of any risks affecting timeline or quality.

5.10 Implementation Timeline

The implementation of the upgraded CAML system shall follow a phased delivery approach with clearly separated deadlines for:

1. Delivery of the upgraded core application (Phase 1); and
2. Development and deployment of newly introduced advanced reporting functionalities (Phase 2).

Phase 1 – Core System Upgrade

The upgraded CAML application, including:

- enhanced case lifecycle monitoring,
- dashboards,
- interoperability components (where feasible),
- data validation mechanisms,
- asset tracking improvements,
- alert mechanisms,
- user interface upgrades,

shall be fully developed, tested, accepted and deployed in the production environment no later than: **30 June 2026**

This deadline shall include successful User Acceptance Testing (UAT) and formal acceptance by the beneficiary institutions.

Phase 2 – Advanced Reporting Modules

The development, configuration and deployment of newly introduced analytical, statistical and strategic reporting modules enabled by the upgraded system shall be completed no later than: **31 December 2026**

These reporting modules shall include:

- enhanced operational statistical reports,
- strategic risk analysis reports,
- configurable international reporting templates (MONEYVAL, FATF, EU),
- cross-instance aggregated analytics,
- exportable machine-readable reporting formats.

The phased approach ensures timely delivery of the operationally upgraded system while allowing sufficient time for refinement, validation and configuration of complex analytical reporting functionalities.

The four (4) basic data-entry training sessions shall be completed before or immediately following production deployment, but no later than 31 July 2026.

Proposed Implementation Timeline (Contractual Version) - exact start date to be confirmed in the contract

Phase	Activity	Estimated Duration
0	Project Initiation & Kick-off	1 week
1	Analysis and Detailed Design	4 weeks
2	Development & Configuration – Phase 1 (Core Upgrade)	3 weeks
3	Integration & Internal Testing (Phase 1)	2 weeks (overlapping)
4	User Acceptance Testing (UAT) – Phase 1	1 week
5	Production Deployment – Phase 1	1 week
6	Advanced Reporting Design (Phase 2)	July 2026
7	Development – Advanced Reporting Modules	Aug – Nov 2026
8	Testing & UAT – Phase 2	December 2026
9	Final Deployment & Acceptance – Phase 2	31 December 2026

5.11 Sustainability and Knowledge Transfer

The Provider shall ensure:

- Transfer of technical knowledge to SPPO IT staff,

- Delivery of system architecture documentation,
- Delivery of database schema documentation,
- Administrative configuration manuals.

The objective is to ensure long-term sustainability and operational independence of the beneficiary institutions.

Full transfer of ownership and intellectual property rights to the SPPO ensures long-term sustainability, independent administration, and institutional control over the upgraded CAML system.