COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 2 November 2021

CDDG(2021)14
Item 3.1 of the agenda

EUROPEAN COMMITTEE ON DEMOCRACY AND GOVERNANCE (CDDG)

DRAFT COMMITTEE OF MINISTERS' GUIDELINES ON THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) IN ELECTORAL PROCESSES IN COUNCIL OF EUROPE MEMBER STATES

Secretariat Memorandum
prepared by the
Directorate General of Democracy
Democratic Governance Division

Introduction

In 2020-2021, the European Committee on Democracy and Governance (CDDG) has been instructed to develop "standards on new technologies and the different stages of the electoral process (including voter registration, transmission and tabulation of results, etc.) in the form of a Committee of Ministers' recommendation or guidelines" (task ii).

To carry out the relevant preparatory work, the CDDG has set up the working group on Democracy and Technology (GT-DT). At its 12th plenary meeting, the CDDG also expressed a clear preference for the preparation of Committee of Ministers' Guidelines rather than a recommendation.

The working group was supported in its tasks by Ms Ardita Driza Maurer, legal expert, Switzerland, as well as Mr Robert Krimmer, ERA-Chair Full Professorship of e-Governance, Skytte Institute, University of Tartu, Estonia and Ms Melanie Volkamer, Full Professorship, Karlsruhe Institute of Technology, Germany.

The working group held four meetings, including informal consultations with election management boards (EMBs) and the Venice Commission. The draft Guidelines on use of ICT in electoral processes were approved in substance during the fifth meeting of the working group on 24 September 2021.

Action required

The CDDG is invited to consider and possibly approve the final draft Guidelines on the use of ICT in the electoral process.

DRAFT COMMITTEE OF MINISTERS' GUIDELINES ON THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) IN ELECTORAL PROCESSES IN COUNCIL OF EUROPE MEMBER STATES

Introduction

Free and fair elections and referendums are one of the cornerstones of democracy. The integrity of the electoral process is fundamental to maintaining public trust in the legitimacy of democratic institutions.

There is a trend to increasingly rely on information and communication technologies (ICT) in all spheres of life, including in election administration. The draft Guidelines aim at contributing to ensuring the integrity of the electoral process and therefore enhancing citizens' trust in democracy. The guidelines identify requirements and safeguards to be introduced in the legislation of Council of Europe member States in order to address the use of ICT in the different stages of the electoral process.

Scope of the draft Guidelines

Countries may choose to use ICT solutions to handle electoral data and processes such as:

- registers and the registering of voters, of observers, of media, etc.;
- the collection of e-signatures in support of questions (e.g., for initiatives or petitions), of candidates, or of parties;
- the internet publication of election-related information;
- the e-transmission of election-data between local, regional and central electoral authorities;
- the online training of election staff and other stakeholders or the e-accreditation of observers;
- the determining, processing, transmitting and publishing of election results;
- the observation of different election related activities, etc.

In addition, ICT solutions have been discussed in the context of the COVID-19 pandemic, as the regular conduct of the electoral process was impacted.

E-data and e-processes may improve the exercise of political rights by offering better accessibility and interaction possibilities, increased transparency, etc. There may also be advantages for election administration, namely speed, efficiency, or accuracy. At the same time, the implementation and use of ICT also increases complexity and heightens exposure to threats and risks inherent in the ICT solutions or systems employed.

The present Guidelines cover the use of ICT solutions by, or on behalf of the relevant electoral authorities, in all the stages of the electoral process, except e-voting and e-counting which are covered by the Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting and are thus out of the scope of the present Guidelines. Hybrid forms of counting, however, which make use of some ICT but do not fall within the definition of e-voting according to the above mentioned Recommendation, are covered by the present draft guidelines. The use of ICT by other actors in the context of the electoral process, namely campaigning activities such as political microtargeting by political parties, or information by media outlets is not covered by the present Guidelines.

Core principles of democratic elections and referendums

The use of ICT, like the use of any other technology in electoral processes, should comply with the principles of democratic elections and referendums and other relevant principles and must be balanced against other core considerations such as security and accessibility for users.

Democratic elections and referendums should be held in accordance with certain principles that lend them their democratic status. The 2002 adopted Code of Good Practice in Electoral Matters of the European Commission for Democracy through Law (Venice Commission),[1] is the reference document of the Council of Europe in the field. It defines the "European Electoral Heritage" through two aspects: the hard-core constitutional principles of electoral law and certain basic conditions necessary for their application.

In line with the 2002 Code of Good Practice in Electoral Matters, the meaning of the core electoral principles and conditions can be summarised as follows:

- *Universal suffrage*: all human beings have the right to vote and to stand for election subject to certain conditions, such as age or nationality;
- *Equal suffrage*: each voter has the same number of votes; each vote has the same weight and equality of opportunity has to be ensured;
- *Free suffrage*: the voter has the right to form and to express his/her opinion in a free manner, without any coercion or undue influence;
- *Secret suffrage*: the voter has the right to vote secretly as an individual, and the state has the duty to protect that right;
- *Direct suffrage*: the ballots cast by the voters directly determine the person(s) elected;
- *Frequency of elections*: elections must be held at regular intervals;
- *Respect for fundamental rights*: democratic elections require respect for human rights, such as freedom of expression, freedom of movement, freedom of assembly, freedom of association;

1 Code of good practice in electoral matters (CDL-AD(2002)023rev2-cor), adopted by Venice Commission at its 52nd session (Venice, 18-19 October 2002)

- *Regulatory levels and stability of electoral law*: rules of electoral law must have at least the rank of a statute; rules on technical matters and detail may be included in regulations of the executive. The fundamental elements of electoral law should not be open to amendment less than one year before an election, or should be written in the constitution or at a level higher than ordinary law;
- *Procedural guarantees*: these include procedural safeguards aiming at ensuring the organisation of elections by an impartial body, the observation of elections by national and international observers, an effective system of appeal among others;
- *Electoral system*: within the respect of the above-mentioned principles, any electoral system may be chosen.

The present draft Guidelines are general and intended for any use of ICT in the considered stages of the electoral process. In addition to core electoral principles and to respect for fundamental rights, the democratic elections and referendums should comply with all other relevant legal principles. These include relevant international obligations, recommendations and standards, namely on elections and ICT, such as those mentioned in the Preamble to Recommendation CM/Rec(2017)5 on standards for e-voting. Furthermore, relevant legal principles are to be found at the national and sub-national levels.

Moreover, security (of the data and the system) should be considered one of the guiding principles that informs the design, development and deployment of ICT solutions at all stages of the electoral process, thus ensuring a security by design approach. For instance, ensuring integrity and authenticity, availability and reliability, secrecy and confidentiality, usability and accessibility, implies that the system and the information are secured against potential risks that would compromise these goals. Hence the assessment of threats should be adjusted to the phase of an election cycle it concerns. Conducting continuous risk management based on predefined criteria for risk acceptance and a predefined methodology is an important part of the effort to ensure security. ICT solutions used should reflect the state of the art and be based on peer-reviewed algorithms and concepts that are broadly endorsed by the respective scientific community. This can enhance trust in the process.

Interdisciplinarity is strongly recommended whenever regulating use of ICT solutions in the electoral process as it positively affects the quality of the regulation. The present draft Guidelines are supported by interdisciplinary research on legal, technical (especially security) and social aspects of the use of ICT in elections. Furthermore, the present guidelines build upon lessons learned from the use of e-voting and e-counting by member States as well as good practice.

General guidelines applicable to all considered stages of the electoral process

In the following guidelines, "Member State" refers to the authority in charge of regulating, conducting or supervising the electoral process in question. Usually, but not always, it refers to the electoral management body, of local, regional or central level. It may also refer to other public authorities like the Parliament or the Government, as the case may be.

1. Member States should ensure that ICT solutions respect the principles of democratic elections and referendums, and that sufficient consideration is given to other relevant principles.

General legal principles that apply to the different phases of the electoral process should be identified. It is often not possible - also with the paper based or manual approach - to implement all principles to the same degree. This could be for two main reasons: (1) There might be a real or perceived conflict between principles (e.g., between secrecy and data protection on one side and transparency on the other) for which a balanced level - to which each of them should be ensured - needs to be defined. (2) Solutions, be it on paper and manual or based on ICT, usually rely on assumptions (e.g., assumptions relating to users' interactions with each other or with the ICT; assumptions on the capability of potential attackers). Only if these assumptions hold, can the principles and derived requirements be ensured. If the assumptions are not realistic, it is very likely that the principles will be compromised and/or violated. Thus, besides identifying the general legal principles that apply, it is important to define the minimum level to which they should be ensured. Furthermore, assumptions should be analysed as part of regular risk assessment (see Guideline 9) and should give sufficient consideration to security concerns.

Detailed and extensive legal and technical requirements that apply to ICT solutions should be derived from the identified legal principles and the corresponding minimum levels to which they should be ensured. The technical requirements should include functional and non-functional requirements (e.g., in addition to security, usability and accessibility requirements also maintenance and interoperability ones) as well as assumptions. For technical requirements it should be indicated which assumptions are acceptable and which are not acceptable (usually because they are not realistic). The definition of minimum levels should include a list of assumptions. The technical requirements and assumptions should be written in a technology-neutral way.

The development and decision process for deducing technical requirements, including minimum levels and assumptions which might be acceptable, should be documented, including information about the people involved (most likely an interdisciplinary team), and be made publicly available, ensuring a transparent process.

Regulation should indicate what complaints and dispute resolution mechanisms are available in relation to the use of ICT solutions and address how to handle possible claims about irregularities.

2. Member States should ensure the usability and the accessibility of ICT solutions used in the electoral process by applying a human centred approach.

Usability criteria for ICT solutions are defined, amongst others, in ISO standard 9241 (2). The user interfaces intended for wider groups of people, especially voters, should be designed following stricter criteria than those intended for small groups of expert users, such as election officials. Accessibility requirement should take user needs into account and ensure that ICT solutions are accessible to all people (whether they have a disability or not). Usability and accessibility thus complement each other. The legal and technical requirements for usability and accessibility and the minimum level to which requirements need to be met should be defined following Guideline 1. The present Guideline 2 deals with the development process.

A human centred approach should be taken when developing ICT solutions for use in the electoral process. This means that from the beginning, (future) users of the ICT solution are involved throughout the entire development and design process. They are involved, for example, through semi-structured interviews, focus groups, via the possibility to provide feedback (on paper) on mock-ups, on processes, and through user studies. A human centred approach also includes the conduct of surveys, once the ICT solution is used in the electoral process, to collect feedback from the field to further improve the usability and accessibility over time.

3. Where member States chose to provide an e-solution which is not universally accessible, an alternative broadly accessible solution should also be provided.

Universal suffrage implies that all electoral stakeholders can accomplish all tasks and exercise all rights, as foreseen by the law. Having a parallel, equivalent procedure, accessible to most users, may be necessary in cases where the ICT solution is not universally accessible. It should also be noted that in some cases the use of ICT can be more accessible to some people than traditional paper-based solutions.

By maintaining an alternative procedure in addition to the ICT one, member States ensure that all stakeholders entitled to universal suffrage have access and thus avoid creating or deepening the digital divide. This implies that potential users are identified, accessibility is assessed, and an alternative and broadly accessible solution is developed and maintained. The public should be informed about the alternative solution.

Regulation should clarify the legal value of the results produced by co-existing alternative solutions as well as the applicable rules in case they are used by the same person. Furthermore, regulation should clarify how to deal with conflicts and other possible issues arising from the use of multiple channels for the same process.

2 https://www.iso.org/standard/52075.html

4. Member states should ensure the integrity and authenticity of the information provided by ICT solutions used in the electoral process. Procedures should be put in place to detect and, if possible, correct any errors or unauthorised intervention.

The ICT solutions should implement authentication mechanisms to avoid unauthorised changes according to the assumptions defined as part of Guideline 1. ICT solutions in the electoral process should operate without errors or unauthorised changes, thus contributing to the integrity of the election. The organisation of the election should provide for accurate checks and balances throughout all relevant election phases. Such integrity checks are essential parts of the overall security and cybersecurity efforts to protect the elections against attacks, from external attackers and/or unauthorised internal access, and of the efforts to address potential mishandling, soft- or hardware errors. Protocols should be in place to detect and respond effectively to such incidents. An appropriate degree of independence for the checks should be provided.

Ideally, any unauthorised changes or errors in the e-process or e-document should be detected and corrected. If that is not possible, corresponding assumptions should be formulated as part of Guideline 1. The possibility to detect and correct errors or manipulations is important in all phases of the electoral process, including when handling voter rolls as well as in respect to tallying and results transmission from polling stations to a regional or central authority, especially if transmission is done via the internet.

Ideally, it should be possible to make someone accountable if unauthorised changes or errors occur. It is essential to provide for an accountable and transparent procedure on how to interact with a running system, correct any data, change or replace a malfunctioning system. Interacting with a running system for such purposes should be addressed in the risk analyses (see Guidelines 1 and 9).

Stakeholders should be able to verify that the tallying and the transmission of results were done correctly, including but not limited to using statistical tests of numerical election results such as risk limiting audits and different types of observations, informed by country specific expertise.

5. Member states should ensure the availability and reliability of the ICT solutions used in the electoral process.

ICT solutions should be available and reliable. The ICT solution should be functional in line with the requirements and assumptions even in the event of system failure, of errors by users or others as well as in case of attacks. Furthermore, the ICT solution should be reliable. It should retain its functionality, irrespective of shortcomings in the hardware or software in other parts of the electoral process. Alternatively, measures should be in place to inform and to activate pre-established fallback solutions and channels, including solutions not relying on active connections.

Incident response and business continuity plans should be put in place and regularly tested. Security measures to ensure availability and reliability include (the list is not exhaustive) management of access rights to the system, procedures for testing the system before the actual election process, procedures for making updates during the operation phase, security rules for transmitting information outside controlled environments, data protection requirements, having the system identify irregularities, informing in case of problems, etc. This may include procedures as required in ISO standards such as the ISO 27000 series.

6. Member states should ensure the secrecy and confidentiality of information stored within the ICT solution, as required by election and data protection laws.

Secrecy and confidentiality requirements derived from the relevant legal principles should be ensured, taking into account the assumptions, which should also be defined, as discussed in Guideline 1. This includes considerations on long-term secrecy, i.e., whether or not secrecy should be provided in time (e.g., given that it is possible to store encrypted data today and decrypt it later, with existing or with new solutions, such as quantum computers which are expected to become broadly available).

Data protection principles such as privacy by design or data minimisation, are minimum requirements and should be considered whenever ICT is used in the electoral process. Furthermore, for each specific ICT solution used, member States should ask the question whether additional, suitable and specific measures, that go beyond data protection ones, are needed to safeguard the fundamental rights of the data subject, as required, for instance, by article 6 paragraph 1 of the Council of Europe Convention for the protection of individuals with regard to the processing of personal data (CETS 108+). If the member State identifies the need for such specific measures, they should become part of the electoral regulation.

Conflicts between transparency on the one hand and confidentiality and secrecy on the other should be carefully considered (see also Guideline 7).

7. Member States should ensure transparency of the election and of the ICT solutions used.

Providing transparency in all aspects of the election is key to a successful and trustworthy conduct of an election, and to promoting trust in the process. Even more so, when ICT solutions are used. Increasingly, non-IT experts experience difficulties understanding ICT solutions. Therefore, there is a need to increase the capacities of all stakeholders regarding understanding the ICT solutions.

All relevant stakeholders should be informed about the use of ICT solutions, including among others about its introduction into the election, its operation, as well as about the post-election assessment of the use of the solution. Information about the introduction includes: 1) elaborating on the overall strategy; 2) publishing technical requirements, assumptions as well as information on how the requirements should be met; 3) addressing perceived shortcoming from previous elections; 4) informing on the development and decision process including the collected inputs as well as on the (interdisciplinary) team involved; 5) informing on the feasibility of the overall implementation; 6) informing on the procurement of the solution and organising it; 7) informing on the exhaustive evaluation before start using the ICT solution as well as informing on the results from the continuous risk assessment; 8) information on how conflicting or competing principles such as privacy and secrecy vs. transparency are to be addressed, 9) publishing the source code, etc.

Transparency also includes providing access to documentation and to the processes to observers, ideally in a language familiar to them.

Further, transparency measures should also include provisions for structured (machine-readable) data about the election process (e.g., location of polling stations, their opening hours, or candidates and election results), including as open data.

Transparency requirements should aim at enabling public scrutiny. Appropriate processes should be in place for receiving, answering or discussing feedback from the public and for processing the conclusions. In this way, transparency can contribute to the overall security and integrity of the electoral process.

Last, transparency is a cross-cutting theme and as such touches on other guidelines as well. It imposes, among others, publishing assumptions (Guideline 1), informing about the development and decision-making process on usability and accessibility criteria (Guideline 2), organising a transparent procedure on how to interact with a running system, correct any data, change or replace a malfunctioning system (Guideline 4), documenting decisions on the availability and reliability, including the respective requirements (Guideline 5), documenting decisions on security and confidentiality, including decisions on reconciling them with transparency requirements (Guideline 6), documenting requirements on system evaluation (Guideline 8), or documenting the risk management process (Guideline 9).

8. Member States should organise an evaluation of the ICT solutions used in the election process by independent experts prior to implementation.

This guideline deals with the process of evaluation prior to implementing an ICT solution in the election process. The evaluation should extend, but not be limited to, security, usability, and accessibility aspects. Its scope should cover the whole ICT solution and its usage environment.

Evaluation approaches should be defined. How to validate that each of the functional and non-functional requirements holds, taking the assumptions into account, i.e., the evaluation assurance level, should be defined. Ideally, preference should be given to a standardised evaluation approach. As a precondition, the target of the evaluation should be clearly defined.

The evaluation requires several documents which, in case of a standardised evaluation, are clearly defined. It should be defined - at a very early stage - whether the evaluation should be conducted only by selected experts who get access to the ICT solution, to the source code, to documentation etc., and/or whether an assessment (or parts of it) can be conducted by everyone because the ICT solution, the source code, the documentation etc., are made publicly available.

It should also be defined how to reach an independent evaluation. The experts should be as independent as possible. This can for instance be reached if two entities are involved: one is mandated to conduct the actual evaluation and the other, a state organisation, supervises the evaluating entity. Different experts might be needed for different requirement areas (e.g., security, usability/accessibility). Finally, it is important to consider the time needed by independent experts to conduct the evaluation.

The evaluation requirements and approach as well as the evaluation results and the people involved (most likely an interdisciplinary team) should be made publicly available.

9. Member States should conduct a continuous risk management of the ICT solutions used in the election process.

Processes important for the correct holding of an election and delivering accurate outcomes might face risks similar to e-voting, in particular if the underlying solution is web-facing. These risks should be managed. In particular, when security risks are identified, proportionate responses should be developed.

Risks should be deduced from the requirements and assumptions (Guideline 1) and the result of the evaluation (Guideline 8). Thus, risk management is relevant during the development process, while using the ICT solution in the electoral process, as well as when preparing future elections. Evaluating the current risks and deciding whether the remaining risks are still acceptable is a continuous process. This is of particular importance as new types of attacks come up over time.

It is important to be aware of the remaining risks. Furthermore, it should be decided whether and if so, how to manage these risks. Risk management approaches should include contingency plans.

In the light of risk management, it should be decided which information should be made publicly available and which not, thereby considering that security by obscurity is generally regarded to be counterproductive.

The risk management approach should be reconsidered on a regular basis, at least after each election. Unusual cases, problems, complaints, etc., should be taken into account.

The risk management approach as well as the people involved (most likely an interdisciplinary team) should be made transparent.

10. Member States should build and retain the necessary capacity to assess, introduce and manage the use of ICT solutions in the electoral process.

When introducing ICT in any part of the electoral cycle, it is necessary that the member States have the necessary administrative and technical capacity and related resources, including financial resources, to plan, implement and run the technology successfully and in a sustainable way.

Member States should consider, among others, the degree of automation of the entire electoral process and potential synergies between the new solution and existing low-, or high-tech ones. Ideally, they have a broader strategy on ICT-related investments.

Administrative and technical capacity essentially requires skilled labour, which should be continuously trained, equipped with the necessary tools and resources, and most importantly, given enough time to focus on their tasks.

The ultimate goal of having the necessary capacities is to avoid outsourcing essential tasks of election administration to third, for-profit, entities and thus enable relevant authorities to effectively oversee the election in accordance with legal requirements, i.e., without being dependent on private parties.

11. Member States should be ultimately responsible, also in cases where private stakeholders are involved.

When organising elections, the member State has the ultimate responsibility for the proper implementation and conduct of the electoral process. This is also the case when third parties (incl. private parties) support the member State in the conduct of the electoral process, or when parts of the electoral processes are outsourced and/or subcontracted to third parties. Third parties have to respect and fulfil the same standards and expectations as member States. Corresponding provisions should be included in the contractual arrangements.

12. Member States should proactively address the possible use of ICT solutions in situations where "force majeure" impacts the regular conduct of elections.

Recent experiences with adapting the electoral procedures to the new health-related restrictions imposed by the COVID19 pandemic have brought forward the question of introducing ICT solutions to help deal with such exceptional circumstances. However, as illustrated by the present guidelines, the use of ICT solutions cannot be considered as a short-term remedy for extraordinary situations. Instead, it should be part of longer-term planning of the electoral process and of a broader approach of dealing with exceptional events.

Member States should proactively address future disruptions, including pandemics. If member States intend to use ICT solution in such extraordinary circumstances, they are advised to prepare in advance for such eventuality, in line with the previously mentioned guidelines.

Glossary of some terms used in the present Guidelines

- **Accessibility:** Accessibility is about designing products and systems that are accessible for everyone, whether they have a disability or not. At the same time, accessibility may specifically address discriminatory aspects related to equivalent user experience, focusing on people with disabilities to ensure inclusion.[3]
- **Assumption**: Assumptions about risks are particularly relevant to security and when security risks are identified, proportionate responses need to be developed. Assumptions can be considered realistic or unrealistic. For instance, with regards to secrecy, it might be assumed that attackers have only certain capabilities (e.g., attacker cannot break the encryption algorithm used), or, with regards to integrity, it might be assumed that honest users will take particular steps to verify the correctness of some functionality. Unrealistic would be for instance to consider that attackers are not able to install key-loggers on voters' devices used to get access to the ICT solution. Assumptions need to hold also in practice for security to be effective. Total security cannot be achieved based on assumptions. However, assumptions contribute to identifying risks and developing proportionate responses.
- **Authenticity** (of the information): The property that data originated from its purported source.[4]
- **Availability**: Ensuring timely and reliable access to and use of information and systems.[5]
- **Elections**: a political election or referendum
- **Human-centred** (design): (as used in ISO standards) is an approach to problem solving, commonly used in design and management frameworks that develops solutions to problems by involving the human perspective in all steps of the problem-solving process. Human involvement typically takes place in observing the problem within context, brainstorming, conceptualizing, developing, and implementing the solution.[6]
- **ICT**: Information and communication technology. In this Guideline, it stands for products and processes that store, retrieve, manipulate, transmit, or receive information electronically in a digital form.
- **Integrity** (of the information): The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.[7]
- **Member State**: In this Guideline, "Member State" refers to the authority in charge of regulating, conducting or supervising the electoral process in question. Usually, but not always, it refers to the electoral management body, of local, regional or central level. It may also refer to other public authorities like the Parliament or the Government, as the case may be.

3 https://www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/
4 https://csrc.nist.gov/glossary/term/authenticity
5 https://csrc.nist.gov/glossary/term/availability
6 https://www.w3.org/WAI/redesign/ucd
7 https://csrc.nist.gov/glossary/term/data_integrity

- **Minimum level** (to which legal principles should be ensured): It is often not possible to ensure the full respect of all principles, among others because there might be conflicting or competing principles such as secrecy and data protection on one side and transparency on the other. In this case a balance of interest must be reached and the minimum level, to which each of the conflicting principles should be ensured, needs to be defined. This decision should be taken by the competent authority, usually the legislator. The essence of the principles cannot be violated.
- **Reliability**: The ability of a system or component to function under stated conditions for a specified period of time.[8]
- **(Technical) Requirement**: A condition or capability that must be met or possessed by a system or system element to satisfy a contract, standard, specification, or other formally imposed documents.[9]
- **(Legal) Requirement**: A legal requirement is a concretisation of a legal principle. For instance, the legal requirements that apply to the transmission of results from polling stations to a central election commission (e.g., on deadlines, formats, checks, etc.) are derived from and are a concretisation of the principles of universal, equal, free and secret suffrage.
- **Risk**: The level of impact on organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.[10]
- **Threat:** Threat is derived from the intent and capability of actors. There are international examples of high capability actors interfering with electoral ICT. Therefore, it should be assumed that there is a high threat to electoral ICT.
- **Usability**: Usability is about designing products to be effective, efficient, and satisfying. It includes user experience design and is closely related to accessibility (11).

8 https://csrc.nist.gov/glossary/term/reliability
9 https://csrc.nist.gov/glossary/term/requirement
10 https://csrc.nist.gov/glossary/term/risk
11 https://www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/