EUROPEAN UNION
ELECTION OBSERVATION

PRACTICAL CORE TEAM GUIDELINES FOR OBSERVING THE USE OF ICTs IN ELECTIONS

Updated March 2025

Introduction

These practical guidelines are designed to help European Union Election Observation Missions (EU EOMs), and EU Election Expert Missions (EEMs), to observe and assess the introduction and use of digital election technologies.

The document is structured in six sections:

1) The first one contextualises the scope of the assessment and briefly introduces the three main technologies that considered for assessment.
2) The second section establishes the international standards against which the missions will assess digital electoral technologies.
3) The third section is based on a regular life cycle of an IT project and determines the concrete aspects or phases to be assessed.
4) The fourth section provides guidance on how to observe the topics presented in the previous chapters. It also provides a practical list of questions that observers could consider when assessing digital election technology.
5) Reporting and drafting recommendations
6) Cooperation with other EU EOM members

1 – Understanding the context: ICT and elections

Scope of the observation

Digital election technology refers here to any computer-based mechanism that substitutes, totally or not, paper-based electoral processes. Digital technologies combine benefits with potential harmful effects. They also require a reconsideration of how principles for democratic elections apply.

While ICTs are now regularly used at all stages of the election process, these guidelines focus on three types of electoral technology that may be implemented both before and after the deployment of the election observation mission: biometric voter registration and identification, electronic voting and results management.

Biometric voter registration and identification

Biometric voter registration is based on the capture of a body-related trait, usually a facial image, a fingerprint or a signature, in order to serve as an identifier for voters on the register. In some cases, the electoral administration is responsible for capturing and registering such data. In other cases, another institution has captured and recorded the data for other purposes, such as civil registration, and the electoral administration uses it as a basis for the creation of a voter register.

Biometric identification in the polling station relies on automated technology to confirm the identity and eligibility of voters by comparing the voter's biometric trait against the biometric information of a set of people included in a poll book.

The use of biometrics intends to enhance the accuracy of voter registration. However, it also brings challenges, such as data protection, logistics, timelines, potential cultural reluctance and the need for adequate training. Biometrics credibility will also be at stake if false positives or negatives exist.

Electronic Voting

Electronic voting uses digital technologies to replace the process of completing and casting a ballot. Two main options exist:

a. voting machines that are used for casting, recording and saving the relevant ballots. Such machines are used in controlled environments (i.e. polling stations or other polling sites for advanced voting schemes)
b. Internet voting mechanisms that serve to cast and transmit the ballot to a remote data server. Internet voting can be used from both controlled or uncontrolled settings.

Electronic voting challenges the traditional understanding of how standards apply to democratic elections, mainly due to the fact that evidence on the integrity of the results is digitally based.

Election Results Management

Election results management is the process by which an election authority counts, tabulates, aggregates, and announces the outcome of an election[1]. Digital technology can be used in all or some of these stages.

For the counting stage and data transmission, a number of options exist:

a. All electronic voting solutions perform the counting and some of them also include the transmission of results.
b. Scanners can be used to count the votes on paper ballots and transmit the results.
c. Paper results forms can be scanned and related data transmitted
d. Data from results forms can be transmitted via other digital tools as well, such as e-mail or text messages.

For the tabulation steps, verification teams check accuracy and consistency of data entries from polling stations. Automatic controls may exist to mitigate errors too. The system should be carefully gauged to support peaks of information in a very short timeframe. Different software and suppliers may be in place.

Digital technology applied to results management enhances accuracy and rapidity, but at the same time interruptions or unexpected delays could be interpreted as a manoeuvre and create a hostile atmosphere. How results are handled can potentially undermine the overall successful conduct of the electoral process.

[1] EC-UNDP Taskforce, *Electoral Results Management Systems: Catalogue of Options. A guide to support electoral administrators and practitioners to evaluate RMS options, benefits and challenges* (2015).

Some technical solutions (e.g. voting machines) may merge all three mechanisms (i.e. biometrics, electronic voting, electronic counting / transmission) that have been discussed above.

At the same time, digital election technologies continue evolving and new options may appear (e.g. blockchain, cloud, quantum). Observers should follow such developments and remain ready to adjust the methodology as needed.

2 – Principles for democratic elections and electoral ICT

With certain exceptions, international and regional instruments are based on a traditional paper-based approach to the conduct of elections. They do not mention digital election technology and therefore their interpretation needs to be adjusted to this reality.

International standards and commitments for democratic elections refer to the key texts used by EOM/EEMs, such as the UN ICCPR and related General Comments (GC). In particular, special attention should be paid at least to:

a. article 25 ICCPR on the right to political participation and the related GC 25
b. article 17 ICCPR on the right to respect of privacy and the related GC 16

When it comes to UN specific conventions[2], all of them may be connected to how digital technologies are applied in elections and how they may impact on the participation of vulnerable groups and on topics covered by UN texts. African, American and European[3] regional organisations also establish principles for democratic elections and they similarly require relevant adjustment when interpreted.

Other entities that are involved in election observation have issued handbooks on observing election technologies, such as OAS (2010), The Carter Center (2012) and OSCE/ODIHR (2013, updated 2024). Finally, in 2022, the community of practitioners working under the umbrella of the Declaration of Principles for International Election Observation developed a paper defining the principles on which the observation of digital election technologies should be based (*General principles and guidelines related to ICT and elections*). Such principles include:

- ***Secret suffrage***

Secrecy prevents the association of a ballot to a specific voter thereby allowing for a free choice. It includes two different aspects:

a. The opportunity to *cast* a ballot without disclosing the content to other persons
b. The impossibility to trace a cast ballot back to a given individual. It refers to *anonymity*.

Regarding the first condition, attention should be paid to remote voting mechanisms (e.g. Internet

[2] CRPD (Persons with Disabilities), CEDAW (Women), UNCAC (Corruption), ICERD (Racial discrimination), ICRMW (Migrant workers), Indigenous and Tribal People

[3] The Council Europe issued certain documents that target digital electoral technologies and some of them belong to the Venice Commission: CoE Recommendation 2017 (5); CoE Guidelines on the use of information and communication technology (ICT) in electoral processes (2022); Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe (2004); Principles for a fundamental rights-compliant use of digital technologies in electoral processes (2020).

voting) and how they manage to ensure both the secrecy of the ballot and the related free cast of a vote. In this regard, comparisons between digital election technologies and remote voting mechanisms, such as postal voting, are useful since both intend to enhance accessibility by implementing special voting arrangements.

Moreover, in order to safeguard the secrecy of the vote and protect against potential coercion of voters in a remote location, some election technologies allow for casting of several ballots and taking only one of them as valid.

In order to guarantee that the voter choice cannot be tracked back to the voter, consideration should be given to systems where voter identification is connected to the mechanism for voting:

a. For local voting machines, logs where ballots are recorded should be randomized so that no match could be done with the chronological sequence of voters
b. For solutions where voter identification and voting mechanisms are embedded in the same device (e.g. Internet voting and machines with biometric authentication), anonymity depends on encryption.

- ***Free suffrage***

The free will of the citizens is ensured when there is no coercion of the voter, but free suffrage also requires an informed choice, which entails at least:

a. freedom from manipulative interferences. When digital tools are used, interfaces should be neutral, that is, with no features (e.g. colour, size, placement, pop-up messages, scroll-downs) that could benefit certain candidates.
b. adequate and appropriate information to proceed with the registration / authentication and with the casting of a ballot.

- ***Universal suffrage***

Universality means citizens have both the right and the opportunity to vote. When applied to candidacy, it means citizens have the option to stand for elections. Restrictions, which may differ for voters and candidates, should be based on reasonable and proportional grounds (e.g. age, nationality).

When digital electoral technologies are in place, different challenges may exist regarding universal suffrage:

a. biometric tools should avoid *false negatives* that may disenfranchise eligible voters
b. voting interfaces / layouts and the relevant software should not exclude eligible *candidates*
c. IT *accessibility / usability* constraints may cause *de facto* disenfranchisement
d. targeted awareness raising initiatives should be organised so that citizens, namely those with limited digital literacy, are informed about specific IT requirements

Contingency measures and alternative paper-based ways to enfranchise eligible citizens should be in place to mitigate such risks.

- ***Equal suffrage***

Each voter should have the same number of votes, which should have the same value. All ballots and candidates should be treated with the same criteria.

Digital technologies may affect this principle in different phases of the process:

a. repeated entries in a biometric voter database could allow for casting more ballots than allowed.
b. during the voting phase, poor performance of the polling staff and/or technical mistakes when conducting the voter authentication could result in overvoting. Moreover, voter authentication may take place with polling stations connected to a central data server, increasing the corresponding challenges.
c. not neutral IT interfaces (e.g. colour, size) could benefit certain candidates.

- **Integrity** of the election

Integrity refers to the accuracy of the results, that is, all ballots coming from eligible voters are properly handled and tallied. They are cast as intended, recorded as cast, counted as cast and no ballots are illegally subtracted. No extra ballots should be added either.

When considering digital technologies, at least the following two topics deserve attention: how to determine the integrity of the ballot box and how to verify that results match the actual will of the voters (integrity of the results).

When it comes to the integrity of the e-ballot box, different IT measures should be used to ensure that it is both empty at the very beginning and secured during the voting period. Such measures comprise the verification of the relevant IT solution in order to avoid malicious software that could add or subtract ballots inadvertently. Moreover, the e-ballot box should be sealed to make sure the same audited version is used in all devices.

Preventing ballot stuffing also requires a proper handling of ID credentials since attackers could access the database and insert ballots. While a reconciliation with the number of voters on the voter lists may be feasible if a separate authentication is in place (e.g. voting machines), other systems (e.g. Internet voting) do not provide such independent evidence and therefore detecting these cases of ballot stuffing relies on how ID credentials are handled and distributed.

Political parties, candidates and other stakeholders (e.g. civic associations, research labs) should have the chance to monitor the integrity of the ballot box in an open and inclusive manner and assess whether the IT measures in place are the appropriate ones to achieve the intended outcome. Computer science skills will be needed since the protection of the e-ballot box is based on IT mechanisms.

The EU EOM's analyst is not supposed to conduct audits or certifications. Findings and recommendations should rely on direct observation of the electoral process. The information received from the EMB and relevant stakeholders as well as the actual professional capacity of such actors should be assessed too.

Regarding the results, election integrity entails a proper handling of the ballots and the chance to conduct recounts, either of ballots and/or results forms. Should paper ballots or paper results forms remain in use (e.g. scanners), traditional recounts could still be performed. Voter Verifiable Paper Audit Trails (VVPAT) for voting machines may also permit a sort of recount by matching electronic results to the ones from the receipts. In all other cases, the integrity of the results relies on sophisticated IT analysis. Criteria above on the different roles of observers and other stakeholders for the integrity of the e-ballot box apply here too.

- **Transparency**

Transparency entails access to information in the sense that enough data are available to ensure that the process is conducted according to procedures. Elections are open to scrutiny by stakeholders, who are able to independently verify the process.

This principle needs a specific understanding when applied to digital electoral technologies mainly because:

a. stakeholders differ with the inclusion of new actors and/or new roles.
b. evidence provided by IT tools have a digital nature and therefore they cannot be understood by most stakeholders.

Besides the usual data that are disclosed in any electoral process, access to digital data, such as the system's configuration and information about its technical preparation, should allow stakeholders to form an opinion on the performance of the IT solution and the extent to which it complies with the standards for democratic elections. Likewise, access to procedural information (e.g. procurement) may be useful to assess the professionalism, ownership and performance of the EMB when dealing with IT tools.

Such disclosure policy should be compatible with concerns and legitimate interests related to intellectual property rights and national or cybersecurity issues.

Finally, consideration should also be given to the fact that certain IT solutions incorporate technical features that enhance transparency by themselves. It is the case of VVPAT for voting machines and E2E verifiability for Internet voting, which serve both as transparency and verification measures.

- **Ownership**

Ownership refers to the institutional capability to conduct a process in a professional, accountable and efficient way. Ownership refers to a variety of institutional aspects, which include:

a. planning capacity in terms of implementation of strategic/operational programmes, needs assessments, feasibility studies, technical specifications or risk evaluations
b. competent EMB units ready to monitor the implementation of IT projects, either internal or outsourced.
c. budgetary resources allocated / distributed accordingly and in timely manner.
d. efficient and clear internal decision-making with the corresponding legal framework

When election IT tools are used, ownership is crucial since outsourcing will likely assume a greater role and therefore EMBs should be able to establish peer relationships with vendors and consultants, which

is only feasible when the EMB has an in-depth understanding of the challenges in place. In this regard, procurement[4] may gain importance as an area of assessment for the expert since it is the way through which private suppliers become involved in the electoral process and liaise with the EMB . Outsourcing may encompass the technical design as such, but also other areas like drafting the needs assessment, conducting the feasibility study or assessing the legal framework.

- **Security**

Digital security means protecting the computer-based systems from external, or even foreign, cyber-attacks, as well as internal errors or sabotage[5]. The umbrella term cyber-hygiene refers to measures that intends to anticipate, prevent and mitigate IT incidents.

In IT security and contrary to paper-based elections, which are mostly decentralized, attacks with devastating effects could be undertaken with much less investment in terms of human or logistic resources. At least four types of IT threats could be considered:

a. attacks to the system (e.g. DDoS), that is, activities that render the IT tool or parts of it not operational, either temporarily or permanently. Such attacks do not affect sensitive data, but they may cause delays or even postponements of election-related activities.
b. attacks to voter registration/authentication causing *de facto* disenfranchisement or leaks of sensitive data.
c. attacks to the accuracy of the results
d. attacks to the secrecy of suffrage (e.g. man-in-the-middle), that is, results are not altered, but some actors gain access to the logs indicating who voted and how.

In the case of an attack, it should be assessed taking into account the following issues:

a. its actual impact on the election process
b. its connection to a particular standard for democratic elections [(e.g. universal suffrage or secret suffrage)]
c. the remedies in place to mitigate or even circumvent the negative consequences
d. the reasons why a country has adopted certain IT tools, the goals to be achieved (e.g. engaging diaspora) and the extent to which all risks have been considered.

IT security also refers to data protection[6]. Secret suffrage is a sensitive issue, but the electoral process relates to others, such as the personal data handled during voter registration and authentication, with special attention to certain groups (e.g. people with disabilities or LGTBI community).

[4] International references on procurement issues may be found at: OECD Recommendations on Public Procurement (2015), a broader one on Public Integrity (2017) and the UN Convention Against Corruption (UNCAC / 2003). Though not as international standard as such, observers may also wish to consult the following very targeted report: *Procurement Aspects of Introducing ICTs solutions in Electoral Processes: The Specific Case of Voter Registration* (2010), which was prepared by EU-UNDP Joint Task Force.

[5] A computer-based system is made up of the applications also referred to as the software, some computer equipment or the hardware, the telecommunications infrastructure and the data that feed them.

[6] International references on data protection include at least the following documents: [1] *UN CCPR General Comment 16* (1988) and *UN Guidelines for the Regulation of Computerized Personal Data Files* (1995) [2] *OECD Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980)

Data protection combines substantial principles (e.g. proportionality, lawful aim, consent, accuracy) with procedural (e.g. right to access, secured data) and institutional (e.g. data agencies) guarantees.

- ***Public trust***

Public trust would be an overarching condition that affects the whole election process in the sense that the outcome should be accepted by the citizens as a result of a credible and genuine process. Public trust is an outcome to achieve (or to maintain and reinforce) rather than a principle or standard.

Certain election technologies pose additional challenges to citizen trust, in particular

a. those that do not provide evidence capable to be understood by laymen, such as e-voting
b. where conclusions based on digital computation are difficult to reverse since providing evidence may be time consuming and not easy to achieve, such as with biometrics.

Observers should assess whether election authorities manage to create a trustworthy environment, with a meaningful oversight system, and how election ICTs impact on such an outcome.

3 – An election technology project: from its adoption until its implementation

This section provides an overview of how an IT project is normally conceived and managed. The text is based on three different dimensions: institutional, technical and civic.

- (A) Institutional dimension / Governance: how governance criteria have been applied to the implementation of digital election technologies. This includes: needs assessment, feasibility studies, legal framework, funding, adoption / planning, in-house / tendering process.
- (B) Technical dimension / IT implementation: different phases that exist in any life cycle of an IT product. Issues include: IT design, technical acceptance / suitability of the product, logistics, end-user training.
- (C) Civic dimension / Confidence building: specific measures should exist to build confidence on a product that will be used to deliver elections. These include: independent audits, sealing ceremonies, simulation exercises.

While the analyst is not supposed to go in depth through all the activities that are described below, such information may be useful background regarding what an IT project entails.

A – The institutional dimension / Governance

Governance refers to the EMB decision-making process through which the project is adopted, developed and implemented. It is connected to the EMB's ownership of the technology, requiring an independent election authority ready to deliver elections in a professional and credible way.

When assessing the governance of an IT project, it is necessary to consider whether the EMB has an internal structure aligned with the complexity of the endeavour, result-oriented procedures established by clear internal regulations and appropriate penalties addressing any malpractices.

Complex IT projects also require competent team leaders and professional IT units. Moreover, the EMB should have a full understanding of the activities to be modified and the actors involved, in particular the ones who are new to an election process, such as IT suppliers and auditors, and how they liaise with the EMB.

From an institutional dimension, attention could be paid to: needs assessment, feasibility studies, legal framework, funding, planning and the in-house development or tendering process.

i — Needs assessment

The needs assessment is the process that should be carried out to determine whether certain areas of the electoral process do not meet the expected outcomes and how they can be addressed. The assessment can produce a structured document or it can be conducted in a more informal way.

In the context of an election reform project, the EMB will likely have completed the needs assessment well before the start of an observation mission. Therefore, the analyst may ask the EMB about how the assessment was carried out and how the need was justified. Such information will provide the analyst with contextual details that will serve to identify the grounds on which the process was launched. Such data may also indicate the actual EMB's ownership of the project, the extent to which the EMB remains the lead actor and the involvement of stakeholders in this preliminary phase.

Possible justifications to introduce the use of technology or to evolve or change an existing solution could include: improving efficiency (getting results soon after voting ends), refining accuracy (avoiding human errors) or achieving more inclusiveness (engaging diaspora).

ii —Feasibility study

A feasibility study is an analysis that considers different factors (e.g. operational, institutional, financial, legal, social, technical) to ascertain the likelihood of completing a project successfully and in time.

The activity will also likely have taken place before the start of the observation mission. Therefore, the analyst will try to obtain information on how it was carried out and the outcome of the study.

iii —Legal framework

The analyst should consider whether the adequate legal basis is in place for the solution and how any legal changes were introduced. The analyst should assess whether such legal framework complies with the standards for democratic elections. Moreover, other issues to consider include:

a) Clarity when using technical terms and whether such approach contributes to the legal certainty
b) The extent to which legal provisions are properly updated to new digital challenges and whether such modifications have been adopted on time considering the long duration of IT projects.
c) The extent to which new provisions at a regulatory level may undermine the role of primary laws for establishing the main legal principles for elections.

iv — Funding

The cost as such is not a primary concern for election observation since it is rather related to a sovereign decision, but other financial aspects may deserve attention. Late disbursements, extraordinary budgetary provisions or insufficient funds, for instance, are indicators to be assessed as they may have an impact on the project execution and the electoral operations. Election technologies may require a sustained process in budgetary terms, that is, instalments to be adopted much beyond the election period as such. When the project relies on external entities, the origin of the funds and the circumstances surrounding the allocation may also be connected to the EMB ownership and

sustainability may be at stake.

v — Adoption and planning

The EMB should define the project planning and governance rules as such, that is, the persons and units responsible for the implementation of the project, its different phases and the reporting mechanisms with the EMB Board. The mission may assess whether the solution is conducive to an efficient and clear outcome compatible with EMB ownership, transparency and accountability.

One of the first steps is to establish the system requirements, which are usually developed by the EMB unit responsible for the process to be computerized. The mission may assess whether they meet the standards for democratic elections (e.g. secret suffrage, universal suffrage). Sometimes, when a problem arises, it becomes apparent that it originated at the very beginning when the technical specifications were drafted and not when they were applied to one specific IT product.

vi — In-house implementation or tendering process

An important decision that the EMB must make is whether to use its own resources or to outsource part or all the activities, which is usual for IT projects, including preparatory tasks (e.g. needs assessment) and/or the actual implementation. Regardless of the actual IT implementation, the EMB should always remain accountable and in control.

With an in-house solution, the analyst may consider assessing the actual EMB institutional awareness on the topic and, as related aspects, the team's capacity to execute the technological project on time, measures implemented to guarantee the quality and security of the IT solution and the extent to which the internal EMB decision-making facilitates the development and implementation of the project.

If the EMB decides to outsource the implementation, the EOM/EEM should refrain from conducting a comprehensive analysis of the tendering process, but should instead pay attention to those aspects that have an impact on the delivery of the elections and how standards for democratic elections are met. Tendering needs competent internal EMB personnel ready to establish sound technical conditions, evaluate bidders and conduct the follow-up in a professional and timely manner. The right to access to public information, which could be used by stakeholders, applies to the tendering process too.

Given that technological solutions often involve contracting several services and projects (e.g. software, telecommunications, hardware), with some of them receiving more public attention than others, the analyst should aim to identify key procurement processes and pay attention to them.

B — The technical dimension / IT implementation

Once a decision has been made on the adoption of a digital technology, a range of technical and operational activities start. The phase comprises different areas such as the technical design of the product, how the solution is verified by the EMB, logistical aspects to be considered for the deployment and finally how to educate future users of the technology.

i – Technical design and integration

This phase intends to achieve a product ready to be deployed according to the specifications and a timeline established beforehand. It encompasses the technical analysis/design as such, the integration of IT components and different security and quality verifications.

This phase usually begins before the arrival of the observation team, but it is quite possible that some activities take place when the mission is already deployed. The analyst may try to obtain relevant information about previous and on-going activities.

Given that the product is still under development, the outcome may not be public and not shared with the EOM. However, the analyst should assess how the principle of transparency applies to this phase and the extent to which such restrictions impact on the standards for democratic elections. In general terms, such a principle does not require access to all data regardless their nature, but at the same time, either during this phase or later on, enough information should be disclosed to the EMB and stakeholders so that they can form a meaningful opinion on the solution.

ii – Technical Assurance and Suitability Verification

Once a working version of the IT product is ready, it is time for the EMB to ensure it meets the specifications (assurance) and responds to the needs that motivated the project (suitability). The EMB should be fully aware of such tasks and have an important role when determining how to conduct them. Information should be shared with candidates and political parties too.

Assurance tests are categorized into functional (i.e. UAT / User Acceptance Test) and non-functional. While the former challenge the product with case scenarios where a user has to get a specific outcome, the latter assess the general conditions under which the product will work, such as a high volume of users or data, its security or usability. Both tests have to be organised well in advance for the implementation team to address any vulnerability.

In parallel, the EMB should assess whether the product suits the needs that were established at the beginning of the project. If it is not the case, the technical specifications may need to be reformulated.

While in some cases the EMB may wish to avoid the involvement of observers, in others it may try to engage them. Observers should be aware that their presence can be instrumentalised. It is important to avoid images or comments that could be misunderstood thereby compromising EOM impartiality. Decisions on whether to accept an invitation will depend on the context, taking account of the public nature of the events, the tasks to be conducted, the role to be assumed or the involvement of other stakeholders. Same cautious criteria apply to other activities below, such as audit, certification or sealing ceremonies.

The mission may request access to the reports proving that these assurance and suitability assessments were carried out. The analyst should also consider feedback from stakeholders, such as political parties, academia or IT think tanks, to evaluate the outcome, rigour, inclusivity and coverage of these activities.

iii – Logistics

Technology must be operational where needed, at the right time and with no interruptions. This means setting up and delivering on time all ICT devices with the same version of the software. When technology is used at field level (e.g. polling sites, voter registration places), hundreds of technological kits need to be assembled and delivered to specific locations while power supply or internet connectivity need to be checked and provided if needed.

The mission may assess the assembling, quality control, transportation, delivery and safe storage of the kits at their destination. Moreover, attention could be paid to contingency or mitigation strategies in case of unexpected incidents. For the decommission process, there could still be aspects to consider, mainly related to data protection and how to sanitize devices (e.g. voting machines, biometric devices, scanners). Access of stakeholders to monitor the whole process is a good indicator.

iv – End-user support (training and voter education)

End-users are voters and all electoral staff using the technology at the different places and stages of the process, such as voter registration stations, polling stations or counting centres. Proper training is needed so that a reliable IT solution does not fail due to the fact that users are not familiar with it.

Electoral staff are often trained through a cascade model, that is, delivering ToT (training of trainers) sessions to people that will replicate the activity throughout the territory later on. Likewise, awareness raising activities are put in place for voters with a range of options including, for instance, pilot initiatives, mock elections, online training platforms, video tutorials or user manuals in paper.

The mission may evaluate the activities aimed at making end-users familiar enough with the new technology. Attention should be paid to the content of such activities, operational aspects (e.g. duration, location, supporting material) and trainers' skills, to name a few.

C – The civic dimension / Confidence building

Any IT project needs to be audited and/or certified, but requirements for such tasks differ when dealing with electoral matters. Their particular features require certain confidence building activities that go beyond what is the standard for other IT products. In this regard, it is crucial that candidates, parties and other stakeholders remain involved and capable to assess the performance of the new technology. It is a civic dimension that complements technical mechanisms.

Beyond the general involvement of stakeholders in the process, three activities in particular may be considered to assess the actual engagement of such actors: independent audits, sealing ceremonies (i.e. how to ensure that the very last version is the one actually used) and simulation exercises.

i – Independent audits

Regardless of whether it is an in-house solution or outsourced, an IT product that is submitted to an independent audit creates an opportunity to build confidence among stakeholders. Sometimes a distinction is made between audit and certification depending on the lead actor, the scope, the moment when the activity takes place or the expected outcome, to name some factors. Here a broad and flexible concept of audit is used. In any case, the audit should be carried out well in advance so that the findings can be considered before the electoral event.

The expert should pay attention to different aspects that confirm that the audit is a meaningful supervision process and not a charade. Important indicators include: the terms (e.g. scope, calendar) under which the audit takes place, the eligibility criteria of the audit firm, whether other interested parties (e.g. political parties, IT research units) are also allowed to perform such verifications and finally the extent to which the recommendations are implemented.

In any case, an independent audit is supposed to enhance the public confidence and therefore the disclosure policy applied to the reports and whether election stakeholders are involved in the entire process are crucial factors. Constraints may exist since valuable information to potential attackers

could be shared, but as stated above, stakeholders should have enough data to form an opinion on the IT solution.

Observers should be aware that auditors will liaise with the contracting authorities and act according to their legal obligations. They may be not allowed to meet and/or share information with the mission.

ii – Sealing ceremonies

The objective of sealing a computer system is to have information of the configuration of the equipment and the version of the running applications. Such data provide all stakeholders with evidence on which to verify that no changes have been made without authorization. The activity is carried out after completing tests and audits. If a vulnerability is identified afterwards or it is necessary to make any changes, the sealing procedure of the new versions or configurations must be repeated.

There may be different sealing sessions for different software components or infrastructures. This must be defined in the schedule of the technological project and be aligned with the timeline of the electoral process.

From a civic perspective, the sealing is a crucial phase since it is the only moment when stakeholders may verify that the IT product to be used is the one that has been tested and audited beforehand. In this regard, criteria to be assessed include the publicity and rigor of the sealing protocols, the extent to which data is documented and information shared about how the sealing is performed, and finally whether the EMB assumes a leading role in this activity.

iii – Simulation exercises

Simulations intend to run all the election day processes that are affected by the technology in a similar way to how they will be executed. This implies not only relying on the same procedures and users, but also using the technology in its final version and configuration.

The expert should assess the context in which the simulations take place and pay attention to different criteria, such as their scope (i.e. topics), representativeness (i.e. size), EMB tasks and the actual engagement of stakeholders through appropriate public events and information sharing.

While simulations are feasible for certain election technologies, voter registration needs other tests since typically it is not conducted during the electoral period and it is not completed in a short period of time. In any case, biometric voter registration should be piloted and conclusions drawn for a full-scale implementation. The analyst should request information on how such exercises were conducted.

4 – How to observe

Assessing digital election technologies requires the collection of data from different interlocutors and observation of their functioning in light of the standards for democratic elections. The section highlights three aspects of the assessment process: reviewing existing documentation, collecting information and direct observation.

4.1. Reading existing documentation

To familiarise with the context in which the technology object of observation will be used, the following documents provide key references:

a) Primary laws (i.e. Constitution and Election Act), mainly the chapters and articles that

describe the processes in which technology is used (if they exist)

b) Secondary legislation or regulations and case-law that develop or clarify some aspects of the processes under observation.
c) Needs assessment, feasibility studies and any other document determining the reasons why the EMB launched the IT project
d) Strategic and operational EMB planning establishing milestones, distribution of tasks, deadlines or contingency plans related to the IT project
e) In case of in-house development, technical documentation related to the IT product
f) In case of outsourcing, available tender documents and in particular technical specifications, administrative provisions and product documentation published by the successful bidder(s).
g) Previous election observation reports and recommendations.
h) Reports published by independent bodies of proven prestige such as anticorruption institutions, universities, think tanks, civic activists or donor agencies.
i) Reports or statements issued by political parties and candidates
j) Press articles that address the context in which the technological project is developed. It is advisable to read articles from different editorial lines and not assume any of the viewpoints.

4.2. Collect information

International standards for democratic elections (see section 2 above), which are the basis for the EOM/EEM analysis, should serve as main guidance to define a list of issues and related details on which to collect information. The following tables suggest topics of interest and concrete questions aligned with the areas of assessment (4.2.1) and with the different technologies to be analysed (4.2.2). Additional questions are proposed for direct observations to be conducted on election day (4.3).

4.2.1. Collect information per area of assessment

The institutional dimension / Governance

Topic	**Suggested questions**
Needs assessment	• Is the decision of using the technology the result of a needs assessment process? • If yes, who, when and how was it performed? • If not, who, when and how was the decision to use the technology taken? • Were stakeholders involved in the consultation process and to which extent? • Was the ICT Unit of the EMB involved or consulted during the process and to which extent? • Was a consensus achieved among stakeholders? • Is the needs assessment report or similar document available to stakeholders?
Feasibility study	• Has the EMB performed a feasibility study? • If yes, is it available for the mission to read? • What were the main conclusions of the report? Which were the main barriers / constraints to consider? • Did the report give a green light for the project implementation?

	• If no, based on what criteria was the use of a specific technology approved? • Were the EMB relevant units (e.g. ICT, training) involved or consulted during the process and to which extent?
Legal framework	• What specific legal documents regulate the use of technology for each relevant process? • Was the legal framework updated to accommodate the use of technology? • If yes, were changes introduced well in advance? • If not, was there a sufficient basis for implementation of the technology? • Was the legal framework in line with the international standards for democratic elections and other specific standards and good practice for ICT?
Funding	• What is the source of funding of the project? • Is the funding adequate for the scope of the expected technological solution? • When was the funding approved and delivered?
Adoption and Planning	• Is the Board of the EMB supervising the implementation of the ICT project in a regular and consistent way? • Is there a Project Manager supervising the ICT project on behalf of the EMB in a regular and consistent way? • Are the technical specifications available to the mission? Do they comply with the standards for democratic elections? • Is there a project schedule and is it followed and updated based on the actual project implementation pace?
In-house implementation	• Has the EMB analysed if they have the necessary human and technical resources to implement the project in-house? • Has the EMB reinforced the team with professionals with relevant skills that they do not have?
Tender process	• Was the Request for Proposal (RFP) dossier published in a public procurement portal? • Was the RFP published well in advance so that the procurement is completed with enough time to execute the technological project and the election preparation operations? • Were the technical specifications suitable, comprehensive and detailed enough? • Is the process transparent enough and do election stakeholders have access to relevant information for monitoring the tender? • Are election stakeholders following the process and, if so, what is their feedback? • Did monitoring mechanisms allowing the EMB to follow-up supplier's activities and retain control over them exist? • Do anti-competition provisions (i.e. vendors lock-in) exist? • Are there any appeals connected to the tendering process? • Are vendors legally committed to a higher due diligence according to international principles on business and human

	rights[7]?

The technical dimension / IT implementation

Technical design and integration	
The annex includes a list that is an example of common documents produced as part of an ICT solution implementation project. The mission is not supposed to perform an analysis of the content of those documents, but their absence would indicate that a poorly documented ICT project exists thereby possibly leading to a poorly implemented one. Besides, future evolution or maintenance of the solution will be at risk if documentation is outdated or non-existent. In addition to such texts and while in the implementation process, questions to address to IT suppliers could include: • Are the vendors providing meaningful information to the EMB unit in charge of supervising the implementation project so that they can control it? • Are the vendors delivering the intermediate and final product(s) in time and in accordance with the contracted scope and quality?	
Technical assurance and suitability verifications	
Governance	• Is the EMB staff running the tests without interference of the ICT provider? • Are the technical assurance tests and the suitability analysis included in the Project schedule? • Is the timeline for conducting the tests aligned with the election calendar? Is there enough time to address deficiencies revealed by the test? • Is there information about the tests shared with stakeholders and to which extent?
Suitability analysis	• Is the EMB conducting a suitability analysis of the IT product vis-à-vis the needs of the project? • Is the outcome of such analysis shared with stakeholders? • Is there a consensus among stakeholders on the suitability of the IT product?
User Acceptance Tests (UAT)	• Is the type, content and number of tests formally established before their initiation? • Is their scope comprehensive enough? • Are the tests executed introducing / loading valid and invalid data sets? • After the User Acceptance Test process, is the EMB delivering a report to the ICT provider detailing the results of the test and prioritizing the deficiencies to be corrected (if any)? • Are the deficiencies duly addressed after the test?

[7] References to such principles include, among others, the UN Guiding Principles on Business & Human Rights (2011) and in particular documents issued by the UN B-Tech Project. Along the same lines, the OECD Guidelines for Multinational Enterprises (2011) and the related OECD Due Diligence Guidance for Responsible Business Conduct (2018).

	• Is there room for a second set of tests to verify the correction of the deficiencies?
Performance, Load and Stress tests.	• Are the Performance, Load and Stress Testing activities included in the Project schedule? • Is their scope comprehensive enough? • Are the metrics defining the expected performance / load / peak load or connections defined in the technical documentation or, when applicable, agreed with the ICT provider? • If as result of the test (any of them) there are deficiencies to be corrected, are they prioritised and, when applicable, duly notified to the ICT provider? • Are the deficiencies duly addressed after the test? • Is there time for a second set of tests to verify the correction of the deficiencies?
Security tests	• Is the Security Testing included in the Project schedule? • Is their scope comprehensive enough? • Are the security goals defined in the technical documentation or, when applicable, agreed with the ICT provider? • If as result of the test there are deficiencies to be corrected, are they prioritised and, when applicable, duly notified to the ICT provider? • Are the deficiencies duly addressed after the test? • Is there room for a second set of tests to verify the correction of the deficiencies?
Logistics	
Planning	• Are the plans known by the actors, achievable and aligned with the election calendar?
Storage of technological devices and peripherals	• Are technological devices and peripherals stored in a secured area? • Are technological devices and peripherals included in an inventory? • Are technological devices and peripherals labelled in a consistent way?
Delivering	• Are technological kits delivered based on a predefined protocol? • Is the delivering process concluded in a timely manner? • If not, were there reasonable contingency and mitigation measures?
Material decommissioning	• Is there a plan to recover from the field the equipment and components? • If yes, is it achievable? • If yes, is the affected staff aware of this protocol?
End-user support (training and voter education)	
Planning	• Is there a milestone such as “Solution ready for training and voter education” in the project calendar?

	• Are the training and voter education calendars aligned with the IT implementation and election timelines?
Training methodology of electoral staff (e.g. EMB officials, polling staff)	• Is there a predefined methodology to deliver the training? Is it comprehensive enough? • Does the evaluation method of trainees ensure competent electoral staff? • What is the percentage of staff actually trained before the event? Are there contingency measures for the remaining staff? • Are substitutes also trained? Are last-minute enrolled staff also trained? • Are user manuals adequate and available on time for training? • Are trainers prepared for training? • Do they remain impartial and objective when delivering training sessions? • Are training premises adequate for training purposes?
Voter education	• Are voter education activities addressing issues related to IT tools included in the operational planning? • Are such activities targeting specific vulnerable groups (e.g. citizens with poor digital literacy)? • Are such activities comprehensive enough (e.g. duration, nationwide, content)? • Are pilots with the IT devices (e.g. voting machines) foreseen?

The civic dimension / Confidence building

Pre-election independent audit	
Tendering process	• Were eligibility criteria to be accepted as an independent auditor public, reasonable and rigorous? • Was the scope (i.e. topics to assess, criteria to use and data available) of the audit meaningful and comprehensive? • Are auditors performing their activities in time and within the scope of the contracted services?
Transparency / Ownership	• Who will be given the relevant audit reports and to which extent (e.g. partial / full disclosure, only conclusions)? • Has the EMB the institutional and IT capability to understand and monitor the audit process, including how to implement its conclusions?
Outcomes and actions post audit	• Were the outcomes of the audit meaningful? • Were the outcomes of the audit taken into account to correct deficiencies and vulnerabilities?
Sealing ceremonies	
Coverage and timing	• Was the sealing of the different software components planned considering the logistics constraints?

	• Was the sealing of the hosting infrastructure planned considering its use during election day? • Were the sealing procedures defined in advanced, documented, and followed during the sealing operations?
Transparency and governance	• Did the sealing protocols include mechanisms to prevent collusion among holders of the crypto keys? • How were the relevant master copy(ies) of the IT product secured? • Were the sealing mechanisms (e.g. protocols, ceremonies) open to auditors, observers and party representatives? • Has the EMB IT skills and institutional capability to understand and monitor the process?
Monitoring	• How did the sealing protocol ensure that all devices are configured with the same IT product? • Are there mechanisms to check the status of the system and the hosting infrastructure? • Is there a system to collect the application and systems logs for the auditors to analyse them in the event of an incident?
Simulation exercises	
Governance and civic engagement	• Is the Simulation exercise included in the Project schedule? • Is the EMB capable to monitor in a meaningful way the simulation exercise and its conclusions? • Are stakeholders involved in the simulation exercise and given information to perform a meaningful oversight? Is the simulation plan shared with them?
Scope	• Is the simulation exercise comprehensive enough regarding the different aspects of the implementation of the IT solution? • Among other issues, is the simulation exercise considering the differences in internet or energy supply coverage, sites security and its implications in logistics both for the deployment of equipment and materials? • Is the simulation exercise representative enough in terms of urban/rural polling stations, high/low connectivity and similar factors defining the diversity of contexts?
Timing	• Is the simulation exercise executed well in advance to correct technical and operational issues?

Candidates and Parties *(in addition to the questions above regarding the involvement of stakeholders in concrete activities that may enhance citizen confidence, other more general questions could also be addressed to candidates and parties regarding their actual involvement in the process)*	• Has the party received an invitation to get familiar with the technological solution(s) in place? • Has the party been involved in solution evaluation activities? • Does the party have ICT experts? • Has the party officially expressed concerns or complaints to the EMB regarding the technological solution?

4.2.2 Collect information per technology

It is possible to select a commercial standard (i.e. off the shelf) product as a starting point for the technological solution used in an electoral process. It is also possible that the solution complies with standardized specifications or takes into account certain good practices in the industry. However, there is no solution that does not require customization to meet the specific needs of a given electoral process. Besides, in case of outsourcing, the use of proprietary solutions adds diverse approaches as the ICT provider could claim confidentiality rights to avoid providing information.

Since each electoral process requires ad-hoc technological solutions, it is not feasible to define a closed list of aspects to be assessed, although a baseline is given for each of the three election technologies addressed in these guidelines. The mission will have to assess the technologies involved and develop an ad-hoc set of questions. Therefore, the following lists of questions are intended to guide the assessment but should not limit or condition it.

Biometric Voter Registration

- What is the process to capture biometric data?
- How are new digital data recorded mapped and aligned with data already recorded in the database? How are mismatches handled?
- How are duplicates handled?

Biometric Voter Identification

- How are the biometric voter lists created?
- What is the process to track biometric voter lists and Voter Identification devices?
- What data is loaded in the Voter Identification devices?
- How is the personal data integrity guaranteed?
- How are the data duplicates managed?
- Are the Voter Identification devices transmitting live data during the voting operations?
- What is the process to delete the data on the Voter Identification devices after voting?
- Are the Voter Identification devices transmitting live data during the voting operations?

Election Results Management

- Is the solution only for transmission or also for data introduction at the Polling Station?
- Is there an alternative transmission procedure for those Polling Stations without internet coverage or power supply?
- Could you provide a flow diagram of the results tabulation process?
- Could you provide the different operation manuals that are used per user's type?

- Could you provide details of the hosting infrastructure?
- Is there a dedicated datacentre / is it cloud-based / is there a Content Delivery Network?
- Could you detail the security measures implemented to guarantee the origin and integrity of the data transmitted from the Polling Station / Intermediate Counting Centres?
- Could you detail the user management implemented? What roles and responsibilities have been defined?
- Could you explain the security measures implemented to guarantee the integrity of the information published in the results portal?
- What are the contingency measures in place to guarantee the availability of the systems in case of an incident, such as a blackout, failing or weak internet connectivity, damage of networking devices or server?
- Is there a Business Continuity Plan (BCP) and a Disaster Continuity Plan?
- Is the BCP considering common natural disasters in the country?
- What are the measures in place to monitor the performance / the integrity of the system?

Electronic Voting

- What is the procedure to identify voters' identity and eligibility?
- How is the secrecy of the vote guaranteed?
- Does the system provide mechanisms for individual verifiability?
- Does the system provide mechanisms for universal verifiability?
- How does the system guarantee the integrity of the electronic ballot box?

4.3. Direct observation of operations

Some aspects of the assessment require direct observation of the activities. These activities likely relate to logistics, end user support (training and voter education), independent audits, sealing ceremonies, simulation exercises and of course all activities performed during the election day and results management. While direct observation of most of these tasks has already been analysed above, the next table pays attention to certain aspects that could be assessed during the election day and subsequent phases.

Election day and results management

Opening	• Have the IT kits (e.g. biometric, voting machines, scanners) been delivered before polling station opening? • Were the IT kits complete? • Have the Polling Station members encountered difficulties to setup the IT kits? • If problems existed, were contingency and mitigation measures applied? Were they consistent, reasonable and efficient? • Have Polling Station members been trained? • Have Polling Station members adhered to the instructions in the law and/or in the relevant manuals? • Have the Polling Station members registered themselves using the biometric kit? • Were party agents and observers present and aware

	of functions related to the IT kits? Was any complaint lodged regarding the IT devices and procedures?
Voting	• Have the Polling Station members identified the voters using the biometric kit and/or used the voting device? • Have the Polling Station members encountered difficulties using such devices? • Are voters aware of how to go through the biometric identification and/or voting procedures? • Were contingency and mitigation measures applied? If so, were they consistent, reasonable and efficient? • Did Polling Station members adhere to the procedures in the law and the relevant manuals? • Were party agents and observers present? Was any complaint lodged regarding the IT devices and procedures?
Closing and Counting	• Did the Polling Station members use the counting device (e.g. voting machine, scanner) for counting purposes? • Have the Polling Station members encountered difficulties using such devices? • Are contingency and mitigation measures applied? If so, are they consistent, reasonable and efficient? • Did Polling Station members adhere to the procedures in the law and the relevant manuals? • How long did the automatic counting take? Was it a reasonable time lapse? • Were party agents and observers present? Was any complaint lodged regarding the IT devices and procedures? • Was VVPAT in place? If so, how was it implemented and what were the criteria in case of mismatch between manual and automatic results?
Results transmission	• Have the results transmission kits been delivered before polling station closing? • Was the results transmission kit complete? • Have the results transmission kit operators / PS members encountered difficulties to setup the kit? • Were there delays in completing the transmission? • Were there issues related with internet connectivity? • Did results transmission kit operators / PS members adhere to the procedures in the law and/or in the relevant manuals? • Were party agents and observers present and aware of functions related to the IT kits? Was any complaint lodged regarding the IT devices and procedures? • Were contingency and mitigation measures applied? If so, were they consistent, reasonable and efficient?
Tabulation	• Are Results Protocols reaching the Results Consolidation Platform (RCP) on a continuous and consistent pace?

	• Are operators introducing data at a continuous and consistent pace? • Is there a Dashboard for the EMB to supervise the RCP activity? • Are there mechanisms for the EMB ICT staff, Auditors, and ICT provider to supervise the hosting infrastructure performance and availability? • Are party agents and observers present and aware of the automatic tabulation procedures? • How is the accuracy of data entries verified and double checked? How is the system preventing human errors / bias? • Was any complaint lodged regarding the IT devices and procedures? • Were contingency and mitigation measures applied? If so, were they consistent, reasonable and efficient?
Publication of the results	• Is the Results portal publishing updated information on a regular basis? • Is the Results portal providing meaningful information?

5 – Reporting and drafting recommendations

Electoral technology is not a separate area of assessment but complements the analysis of others such as legal framework, election administration, voter registration, voting and counting, and the tabulation and publication of results. For this reason, devoting a specific section to electoral technology in the preliminary statement and the final report is a decision that should be based on the relevance of technology, such as its introduction for the first time. The final structure of the reports will be determined by the DCO in consultation with EEAS (Democracy and Electoral Observation division).

When it comes to drafting recommendations, the approach should be consistent with the role and mandate of the election observation mission. The EU EOM will have collected information coming from different angles related to the implementation of digital election technologies, but compliance with standards for democratic elections should remain the main guiding principle for drafting recommendations.

For instance, while IT project management issues or preparatory technical tests are interesting and useful for getting the full picture of the project, it may not be appropriate grounds for recommendations unless it has a direct impact on the electoral process, as well as on the standards as such.

Likewise, typically, the EOM will not address recommendations to the vendor. The EMB instead will be the interlocutor for issues related to the implementation of the IT project. All recommendations should be clear, concise and feasible, given the context.

EU EOM recommendations related to election technologies may address topics such as: the transparency of the process, the actual involvement of election stakeholders in decision-making and confidence-building measures or how the principles of secret and universal suffrage are ensured, to name a few. In general terms, when it comes to digital election technologies, trust is a key parameter.

IT tools require new ways to create and consolidate public confidence and the EOM may assess the extent to which such measures succeeded.

At the same time, EU missions should be mindful of certain "red lines" of what should be avoided when developing recommendations. These include:

- A recommendation to introduce specific election technologies
- A recommendation that would fall outside the mission's mandate and whose objective cannot be directly linked with the electoral process
- A recommendation that is not discussed or is not supported/acknowledged as desirable by at least some national stakeholders
- A recommendation that is either overly specific or too vague, posing a risk of misinterpretation

6 – Cooperation with other EU EOM members

The guidelines intend to be useful for different EOM formats, that is, with or without a specific CT position for the analysis of digital electoral technologies and regardless of the concrete background of such an expert (e.g. IT, political science, management, legal, practitioner).

When assessing digital electoral technologies, it is necessary to combine technical inputs with other considerations related to legal, institutional and social aspects. While such assessments cover electoral processes and not the technologies as such, having knowledge of good practices in the use of ICTs, their security and/or their legal requirements, to name few aspects, will allow some aspects to be analysed in greater depth.

Legal Analyst / Electoral Analyst / Political Analyst

These three positions together with the expert on digital election technologies support each other providing complementary views. If no specific position exists for digital technologies and upon decision of the DCO, the Election Analyst may take the lead on the topics discussed by these guidelines.

While the Legal Analyst will contribute with the assessment of the laws and regulations dealing with IT tools, the Political Analyst pays attention to how such mechanisms are perceived by candidates and political parties. Digital technology may easily become a matter for the election campaign and gain prominence from a partisan point of view. Finally, the Electoral Analyst, with or without a specific position in the Core Team for an Election Technology Analyst, will cover aspects related to the election administration, that is, how the EMB conducted its decision-making process.

Data Analyst

Analysing the results of the election to identify trends, correlations or any relationship between the disaggregated results is an activity that is frequently carried out by the Data Analyst. However, the level of analysis depends on the feasibility of obtaining the results in a format that is exploitable by data processing tools, as well as the timeframe for the deployment of the Data Analyst.

The expertise of the Data Analyst contributes to the evaluation of the Results Management System. The observation mission can assess whether the system is conducive to transparency and favours confidence in the electoral process based on the quantity and quality of the data that it allows for

downloading, the format in which it is provided and its level of disaggregation.

LTOs/STOs

LTOs support the observation activities throughout the territory during the weeks prior to election day. In the context of the observation of election technology, their feedback is essential to know if the training activities for poll workers and support officers cover how to use the technological equipment and how effective is this training. The LTO Coordinator should be prepared to highlight these aspects, answer questions or forward them to the Election Technologies Analyst.

In addition, LTOs provide feedback on the logistics associated with the deployment of the technological kits as well as the readiness of the polling places in terms of internet coverage and power supply.

They also assess the simulation exercises in their area of observation considering the organization of the test, the skills of the participating staff, the availability of technological kits and the readiness of the premises. Finally, they retrieve information on how voter registration as well as voter education related to IT tools was conducted in their area of observation.

On election day, LTOs and STOs provide feedback on how technology is used in the voter identification, voting, vote counting and results transmission processes mainly through the observation forms. The tabulation process, either at regional centres or headquarters, also deserves attention since concerns may exist on how digital tools are used to process data entries from the field. Specific LTO and STO teams may be necessary to cover such phases that may last hours or days after closing of the polling stations.

National staff

Observing election technology requires understanding the IT solution in place and contextualizing how it is used. These are activities that an analyst can hardly divide or delegate and, from this viewpoint, the benefits of a national assistant, unless there is a need for interpretation, are limited.

On the other hand, this area of observation involves different aspects that need a plurality of methodologies and a national staff may serve to complete the skillset already provided by Core Team members. In this regard, recommended profiles could target assistants:

A) knowledgeable in computer systems or in ICT security, since this is the field that usually causes the greatest concern among stakeholders and it is rare to have this expertise among the members of an observation mission.
B) familiar in electoral processes when the expert is strong in ICT knowledge but limited elections wise
C) ready to support with IT technical inputs an expert that has a legal or institutional approach to digital election technologies

ANNEX
Implementation documents

Solution Analysis & Design documents:

- Functional Requirements Document(s)
- Non-functional Requirements Document(s)
- Functional Specifications Document(s)
- Technical Design Document(s)
- Wireframes and mock-ups of the user interface products

Solution development documents:

- Testing Methodology
- Quality Assurance reports
- Unit testing coverage reports
- Integration testing coverage reports

Hosting infrastructure documents:

- IT architecture
- Network diagrams

Business Continuity documents:

- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Incident Response Plan (IRP)