General Principles and Guidelines Related to ICT and Elections

A DoP Technical Document
Endorsed by the DoP Implementation Meeting
on December 8, 2022

Following an inclusive review and discussion of Draft Guideline documents, the DoP organizations recognise the Guidelines as Technical Documents to aid the implementation of the Declaration of Principles. They do not require action by the political bodies of endorsing organizations (such as assemblies, councils, or boards of directors), though such actions are welcome.

Table of Contents

Introduction

The opportunities and the risks involved in the introduction and use of new electoral Information and Communication Technologies (e-ICTs) have garnered considerable attention in recent years. Technological progress has resulted in an increasingly wide array of e-ICT solutions being available to automatize specific parts of the electoral process. Their adoption and use has highlighted both the genuinely positive contributions e-ICTs can offer, but also the need for e-ICTs to be solidly grounded on an adequate legal and operational framework that guarantees their principled and efficient application.[1]

In this document, "e-ICT" refers to any digital process that substitutes for manual electoral processes, including technologies for voter and candidate registration, voting, counting and results management. E-ICT processes discussed here do not include the use of internet or social media platforms for political purposes, which constitute a separate topic.[2]

The community of organisations endorsing the Declaration of Principles for International Election Observation (DoP),[3] has the mission to support and enhance the integrity of the electoral process, as well as to promote public confidence in it. As part of this mission, the DoP community considers it important at this moment to highlight what are the key principles that should underpin e-ICT systems. In this context, it is also useful to identify and clarify the responsibilities of all electoral stakeholders towards the adoption and implementation of e-ICTs.

E-ICT systems are subject to the key principles underpinning democratic elections, contained in the International Bill of Human Rights (which includes the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights and the International Covenant on Civil and Political Rights, including its two Optional Protocols), together with other international and regional commitments. These principles should guide not only the design of the systems but also their adoption, deployment and use. As these systems are tools designed to substitute for some of the traditionally manual functions in the

[1] The 2019 'UN Report of the Secretary-General on Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization' underlines: "The United Nations neither encourages Member States to introduce digital innovations in their operational processes nor discourages them. Their potential for increasing participation, reducing certain irregularities and strengthening public trust can be great. At the same time, some of the sobering conclusions outlined in previous reports have been confirmed by recent experience. Those include the importance of ensuring, first and foremost, clarity about the problem to be resolved through any new technology, of taking ample time to consider the technical, financial and political feasibility of the innovation through a broad consultative process and of gradually introducing new technology to allow for thorough testing and adjustment. Such testing should also take into account increasing concerns regarding the vulnerability of national electoral infrastructures to cyberattacks." https://dppa.un.org/sites/default/files/sg-electoral_assistance_report_final_20191114_e.pdf.

[2] The 2019 'UN Report of the Secretary-General on Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization' also makes a deliberate distinction between the influence of the internet and social media and digital technologies for electoral operations. https://dppa.un.org/sites/default/files/sg-electoral_assistance_report_final_20191114_e.pdf.

[3] 'Declaration of Principles for International Observation', endorsed 27.10.2005 at the UN. Currently endorsed by 55 election observer organisations. https://aceproject.org/electoral-advice/dop/the-declaration-of-principles/

electoral process, they should therefore adhere to the standards that apply to democratic elections, namely the integrity, secrecy, universality and equality of the vote, transparency, accountability and public confidence and trust in the election. Given the critical nature of ICT infrastructure connected to elections and the vast amount of data generated, the security of e-ICTs and the need to ensure the right to privacy are also crucial to the integrity of the process. Only by ensuring that e-ICT systems abide by these principles will election management bodies (EMBs) and other stakeholders be able to reap the potential benefits of e-ICTs, thus strengthening public trust.

States, through their EMBs, are ultimately accountable for the credibility of an election, including the adoption and implementation of e-ICT tools.[4] There is, however, emerging consensus that e-ICT vendors also bear responsibilities with regard to respect for fundamental freedoms and human rights associated with electoral processes. Among others, the UN Guiding Principles on Business and Human Rights[5] and the UN Secretary General's High-level Panel on Digital Cooperation[6] have developed a vision for further work on this.

Finally, donors and electoral assistance providers should promote and work to ensure these principles when considering support for electoral processes that involve the adoption of e-ICT systems.

This document provides a set of general principles and guidelines intended to support work by the various communities working in the field of ICT and elections. These include policy makers considering the introduction of ICTs in their elections, EMBs seeking to implement ICT solutions, vendors of ICT electoral solutions as well as observers and other stakeholders in the election process.

The DoP community, as a network of organizations with extensive expertise in the field of good practice in elections, offers these general guidelines as a contribution to all stakeholders.[7] On the basis of these general guidelines, the DoP community intends to offer recommendations directed particularly toward observer organizations, EMBs, legislators/regulators and the donor community.

[4] 'Recommendation Rec(2017)5 of the Committee of Ministers of the Council of Europe to member states on standards for e-voting': https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f.
[5] Business enterprises have a human rights due diligence. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. Office of the UN High Commissioner for Human Rights, 'Guiding principles on business and human rights'. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf . See also the 'Council of Europe recommendation CM/Rec (2016)3 of the Committee of Ministers to member states on Human Rights and Business': https://edoc.coe.int/en/fundamental-freedoms/7302-human-rights-and-business-recommendation-cmrec20163-of-the-committee-of-ministers-to-member-states.html .
[6] 'Report of the UN Secretary General's High-level Panel on Digital Cooperation, the age of digital interdependence', p.16. HLP on Digital Cooperation Report Executive Summary - ENG (un.org)
[7] For a list of documents addressing e-ICTs from DoP endorsing organisations, please see footnote 17.

"[A]t its root, electoral integrity is a political problem. [...] [It] depends on public confidence in electoral and political processes. It is not enough to reform institutions; citizens need to be convinced that changes are real and deserve their confidence. Inclusiveness, transparency and accountability are all fundamental to developing that confidence."[8]

E-ICTs, if implemented correctly, can facilitate efficient and credible management of different aspects of the election process, for instance in voter registration, voting and results management. They can be tools for broader inclusion of voters, enhanced transparency of the process, and new means of monitoring the work of the election administration. However, they can also subvert electoral integrity through technology failure, malign manipulation or a rushed adoption process, or create challenges and increased complexity, thus leading at times to the undermining of a key factor in the election process: trust.

A genuine election is one in which the outcome reflects the freely expressed choices of the people.[9] Political trust – the belief in the integrity of political institutions and the regime of which they are a part – is a critical indicator of political legitimacy. Overall trust in the legitimacy of the election administration is a necessary condition for trust in the integrity of an election. Public confidence is an essential building block for the use of e-ICTs. An incremental approach to their introduction, together with thorough testing, verifiability and full transparency, can help develop public confidence in e-ICT solutions.[10]

Where a significant level of distrust or dissatisfaction with the election administration exists, the introduction of e-ICTs may be problematic and may further diminish public confidence in elections. The adoption of e-ICTs cannot solve political problems that may contribute to the lack of trust in the integrity of an election. Therefore, managing the expectations of what could be the potential benefits of adopting a new e-ICT system should be carefully and independently weighted. All stakeholders, including political parties, have a shared responsibility not to undermine trust in e-ICT systems if good practices have been followed in their introduction and implementation.

The High-Level Panel on Digital Cooperation, appointed by the UN Secretary General in 2018, stated: "There is an urgent need to examine how time-honored human rights frameworks and conventions – and the obligations that flow from those commitments – can guide actions and policies relating to digital cooperation and digital technology." The panel urged the UN Secretary General to begin a process that invites views from all stakeholders on how human rights can be

---

[8] Global Commission on Elections, Democracy and Security, 'Deepening Democracy: A Strategy for Improving the Integrity of Elections Worldwide' (2012), para. 28/29.

[9]' Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization: report of the Secretary-General' (2017) A/72/260, para. 28. https://digitallibrary.un.org/record/1302192?ln=en
Halff, Maarten. 2015. 'Confidence in elections and the acceptance of results. A policy brief of the Electoral Integrity Initiative'. Geneva: Kofi Annan Foundation.
https://www.kofiannanfoundation.org/app/uploads/2016/06/Confidence-in-elections-and-the-acceptance-of-results.pdf

[10] OSCE/ODIHR 'Handbook for the observation of new voting technologies': https://www.osce.org/odihr/elections/104939.

meaningfully applied to ensure that no gaps in protection are caused by new and emerging digital technologies. Its report noted that while states are duty-bound to protect rights and provide remedies, there is also a growing responsibility on the private sector to evaluate risk and assess the impact of their actions on human rights. More recently in December 2020, Council of Europe's Venice Commission has adopted principles[11] which should be respected by law-makers, regulators and other actors involved in the use of digital technologies in elections, which emphasise the need for a human rights-compliant approach; human rights and fundamental freedoms must be translated into the digital environment.

As already mentioned above, the fundamental principles underpinning democratic elections apply to them, namely the integrity, secrecy of the ballot, universality/inclusivity and equality of the vote, transparency, accountability and public confidence (trust) in the process.

The Global Commission on Elections, Democracy and Security underlined the importance of transparency, accountability and public trust as most immediately relevant to the integrity of an election.

Transparency of e-ICT systems has been a prominent concern and a challenge for electoral stakeholders. The systems have often proved to be "black boxes", out of public scrutiny, making it hard to know whether the will of voters is faithfully reflected in election results. A lack of inclusivity in the electoral process, including in key debates and decisions around the adoption of e-ICT have a negative impact on the overall transparency of the process. Equally, a lack of clear accountability in the use of e-ICT systems poses a serious challenge to transparency and credibility. Should results be challenged, national courts will also require insights into the intricacies and functioning of e-ICTs. Verifiability and evidence should be well defined to help courts to resolve electoral disputes in a quick and confidence-building manner. Some fundamental principles can be embedded in the design of a system, making it more likely they will be respected when the system is operating. It is important, then, that commercial providers also view these principles when considering the production of new e-ICT systems.

Principles for genuine elections and electoral ICT

The DoP states that international election observation is an expression of the interest of the international community in supporting democratic elections as part of democratic development, including respect for human rights and the rule of law. It can enhance the integrity of election processes by deterring and exposing irregularities and fraud and by providing recommendations for improving electoral processes. It can promote public confidence, as warranted, promote electoral participation and mitigate the potential for election-related conflict. It also serves to enhance international understanding through the sharing of experiences and information about democratic development.

[11] Venice Commission, 'Principles for a fundamental rights-compliant use of digital technologies in electoral processes'. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2020)037-e

The DoP community represents a constellation of international, intergovernmental, regional and non-profit organisations, each with a different mandate and geographical scope. Celebrated at the United Nations in 2005, the DoP, together with the Code of Conduct for International Election Observers, establishes the basis for credible international election observation and is now endorsed by 55 intergovernmental and international organisations[12] engaged in improving international election observation. By endorsing the declaration, signatories endorsing organisations share the values at the heart of democratic elections and of independent international election observation. One of the roles that the DoP community plays is to consider emerging trends such as the introduction of e-ICTs in elections.

Upholding international obligations and commitments for inclusive democratic elections

Genuine democratic elections encompass a wide range of human rights and fundamental freedoms that should be exercised on an ongoing basis without discrimination based on race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, disabilities, sexual orientation and gender identity and without arbitrary and unreasonable restrictions.

The principles of genuine democratic elections are set forth in the International Bill of Human Rights, supplemented by other international and regional treaties and instruments. This legal corpus includes other human rights – for example the right to privacy - that, while not themselves explicitly electoral in nature, are relevant when considering elections as broad, participatory and inclusive cyclical processes rather than single events.[13]

Secrecy, integrity and security, universality and equality of the vote, transparency, accountability and public confidence (trust) in the process are the basic principles for the assessment of an election. The Global Commission on Elections, Democracy and Security describes an election with integrity as "any election that is based on the democratic principles of universal suffrage and political equality as reflected in international standards and agreements, and is professional, impartial, and transparent in its preparation and administration throughout the electoral cycle."[14] Some DoP endorsing organisations[15] have developed methodologies for

[12] https://www.ndi.org/declaration_endorsing_orgs
[13] Office of the High Commissioner for Human Rights and The Carter Center, 'Human Rights and Election Standards A Plan of Action'(2017).
https://www.ohchr.org/Documents/Issues/Democracy/Elections/POA_EN.pdf
[14] Global Commission on Elections, democracy and security report (2012) "Deepening democracy, a strategy for improving the integrity of elections worldwide."deepening_democracy_0.pdf (kofiannanfoundation.org)
[15] See, for example, OSCE/ODIHR, 'Handbook for the observation of new voting technologies' (2013).
https://www.osce.org/odihr/elections/104939,
Council of Europe 'Recommendations on standards for e-voting'
https://www.coe.int/en/web/electoral%20-assistance/e-votingNational Democratic Institute, 'Monitoring electronic technologies in electoral processes' (2007),
https://www.ndi.org/sites/default/files/2267_elections_manuals_monitoringtech_0.pdf
Organization of American States, 'Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions' https://www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf

observing the use of e-ICTs as part of the electoral process based on these principles.

Following is a brief overview of these principles:

Secrecy of the vote

Secrecy of the vote is at the heart of a democratic election process, and any voting, counting and tabulation process that does not meet this commitment would see its credibility reduced, depending on the magnitude of the non-compliance. Secrecy of the vote means it should not be possible to associate a vote with a specific voter, which permits the voter to exercise her or his choice freely, without the potential for coercion, intimidation or vote-buying.

For e-ICT systems associated with voter registration, the principle applies to the treatment of voters' personal data, its privacy and measures taken to ensure it is used only for the purposes prescribed by law.[16] Privacy International has identified the following conditions for access to data contained in voter register based on data protection principles and best practices:[17] the voter register should not include personal data other than that which is required to establish eligibility to vote; the law should define the minimum standards of security to protect the voter register against unauthorised access; it should also define the conditions and limits of access to the data contained in the voter register; personal data from the voter register should not be public by default; if there is to be an open register which anyone can buy access to for any purpose, this should operate on an opt-in as opposed to opt-out basis; it should be made clear in law and in relevant guidelines that personal data from the voter register which have been made accessible are still subject to, and protected by, data protection law, including for onwards processing; access to and use of personal data contained in a voter register should be regulated; and who is entitled to access and for what purposes should be clearly stipulated in the law, limited to what is necessary for the electoral process, with clear prohibitions on using this data for any other purpose.

Integrity of the Vote

Accurate counting of votes and reporting of results implies a chain of actions. All votes must be cast as intended, and must be counted as cast, with no votes illegally added or subtracted. Voters need to be certain that votes are cast and accounted for without modifications. The security of the result management system must ensure there is no possibility for undetected fraud or error to alter the results. In a paper ballot system, the integrity of this chain can be ensured through observation of each step of the process[18] and verification, if necessary and allowed

[16] In the EU (and the EEA) data protection and privacy are regulated by the General Data Protection Regulation (2016/679), which applies in the context of an election. Additional elements specific to elections were added by the European Data Protection Board before the recent European Parliament elections in 2019 (EDPB, Statement 2/2019) and by the Council of Europe with the (2018), 'Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data'.

[17] Privacy International, 'Technology, data and elections: A "checklist" on the election cycle', https://privacyinternational.org/advocacy/3093/technology-data-and-elections-checklist-election-cycle

[18] Although in some cases this is not fully possible for all stakeholders, for instance with postal voting, where integrity relies on the assumption of the safety and reliability of the postal service.

by legislation, through the possibility of a manual recount. E-ICTs are subject to the same requirements.

Equality of the Vote

Equality of the vote means no voter can cast more votes than another. E-ICT systems must prevent any person from casting more votes than is established by law and must prevent votes from being subtracted from the system. Some e-voting systems allow voters to cast their vote more than once, with the condition that only the last cast vote is counted. This helps reduce the risk of voter coercion and vote-buying. Consequently, it must be possible to verify that no violations of the principle of equality have taken place.

Universal Suffrage

Universal suffrage means all eligible adult citizens must have the opportunity to vote and that effective means for their participation should be provided. In this respect, E-ICT systems have a great potential to enhance accessibility to suffrage to voters facing obstacles in the exercise of their right to vote.

Transparency

A transparent election process is one in which every step is open to scrutiny by stakeholders (political parties, election observers, the media, courts and voters), who are able to independently verify that the process is conducted according to procedures and without irregularities. Providing transparency in an election helps establish trust and public confidence in the process, as voters have a means to verify that the results are an accurate reflection of the will of the people. The UN General Assembly reiterated[19] that "…transparency is a fundamental basis to the accountability of Governments to their citizens, which, in turn, is an underpinning of democratic societies."

The Council of Europe is so far the only[20] organisation to have adopted intergovernmental standards on e-voting.[21] The recommendation also includes standards on transparency and observation, making it clear that "any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results."

Applied to the specifics of e-voting, the Council of Europe in 2017 called on Member States to be transparent in all aspects. "The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple

---

See for instance Venice Commission, 'Report On the compatibility of remote voting and electronic voting with the Standards of the Council of Europe'. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)012-e .

[19] United Nations Resolution on 'Strengthening the role of the United Nations in enhancing periodic and genuine election and the promotion of democratisation', (2019) A/RES/74/158. https://digitallibrary.un.org/record/3847788?ln=en

[20] The US has adopted the 'Voluntary Voting System Guidelines', a set of specifications and requirements against which voting systems can be tested to determine if the systems meet required standards. https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

[21] The recommendation was adopted on 14 June 2017 and is complemented by the 'Guidelines on the implementation of the provisions of the recommendation with specific requirements' and the explanatory memorandum'. https://www.coe.int/en/web/electoral-assistance/e-voting

language, about: any steps a voter may have to take in order to participate and vote; the correct use and functioning of an e-voting system; the e-voting timetable, including all stages." Moreover, "the components of the e-voting system shall be disclosed for verification and certification purposes."[22]

Before technologies are introduced, consultations should take place with key stakeholders on why e-ICT solutions are being proposed, how they might address specific challenges and improve the electoral process, as well as what they cannot achieve and their associated risks and plans to mitigate them. These issues should be explained clearly to the media and to citizen observers from the very start of the process of adopting e-ICT.[23] Transparency of the procurement process is also essential for accountability, consensus and trust. In cases where external support is provided, clear criteria and recommendations should be set by key donors, not least since procurement may be covered by funding intended for democracy support and electoral assistance.[24] It is also recommended that national stakeholders, including contestants, media and civil society, are given the opportunity for meaningful input into and monitoring of the introduction and implementation of such systems.[25]

Defining who is best placed to promote, assess and verify the principle of transparency is an important issue, and is a question related to some extent to the principle of accountability. While electoral contestants and observers have a critical role to play in promoting the transparency of an election process, it is ultimately up to the EMB to ensure this principle is respected.

E-ICT systems often require a certain degree of expertise to fully understand them; however, the principle of transparency requires that e-ICT systems do not prevent individuals from scrutinising and understanding election results, even without specialist technical knowledge. In some countries there are specific requirements on adherence to this principle, as exemplified by the judgement of

---

[22] 'Recommendation Rec(2017)5 of the Committee of Ministers to member states on standards for e-voting': https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

[23] 'UN Report of the Secretary-General on Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization' (2019) A/74/285, para 38. https://dppa.un.org/sites/default/files/sg-electoral_assistance_report_final_20191114_e.pdf

[24] For instance, the EU recommendations on procurement include: "Check which solutions and license are already available for re-use purposes; request functionalities to make data transfer effective; request ICT solutions to be easily accessible by everybody; avoid referring to proprietary products such as: brand names, trademarks and patents; do not request solutions with features that go beyond what is necessary; and assess the public procurement exercise." See EU 'Guidelines on procuring IT solutions': https://joinup.ec.europa.eu/collection/eprocurement/discussion/guidelines-procuring-it-solutions. Additional references to European Commission decisions in a procurement context: 'Against lock-in: building open ICT systems by making better use of standards in public procurement', COM (2013) 455 final, p.4.; 'Guideline on public procurement of open source software' (2010), p.42, 56. 'Guide for the procurement of standards-based ICT — Elements of Good Practice' SWD (2013)224 final, p.33.

[25] DoP, Para 16, "Citizens have an internationally recognised right to associate and a right to participate in governmental and public affairs in their country. These rights may be exercised through nongovernmental organisations monitoring all processes related to elections and observing procedures, including among other things the functioning of electronic and other electoral technologies inside polling stations, counting centers and other electoral facilities, as well as the transport of ballots and other sensitive materials..."

the German federal court on the use of voting machines.[26] In the opinion of the court, transparency is guaranteed only if "the essential steps of voting and tabulation of results can be examined reliably and without any specialist knowledge of the subject."

It is therefore essential that an EMB fosters an environment that grants all electoral stakeholders access to the process in order to carry out a meaningful observation, either directly or via technical experts.[27] The Council of Europe guidelines accompanying its Recommendation, for instance, make it clear that "observers, including representatives of political parties and the general public, should be granted access to all relevant information during the entire duration of the certification process in order to carry out their duty." Furthermore, the Explanatory Memorandum to the Recommendation underlines that "observers, to the extent permitted by law, should be able to verify that the e-voting system itself is designed and operated in a way which respects the fundamental principles of democratic elections and referendums. Therefore, States should have clear legal provisions on observers' access to the e-voting system documentation and audit data."[28]

In this respect, it is also important to note that intellectual property and trade secrecy should not be used as justifications to thwart the principle of transparency. This is a recurrent issue when digital solutions are employed for the performance of public services and it has increasingly been recognised that safeguards should be in place to limit the capacity of companies and governments to use intellectual property or trade secrecy as a way to shield themselves from scrutiny.

The use of e-ICTs entail a number of other activities, some critical to the integrity of the process, that can be observed but which take place well in advance of election day. These include the testing and certification of the systems and the installation of software. Any verification/auditing process should be led by national actors and guided by independent experts selected in an inclusive and transparent process. EMBs should ensure transparency by providing information on the testing and certification of e-ICT systems, something clearly set out in the DoP: "[The EMB] guarantees unimpeded access of the international election observer mission to all stages of the election process and all election technologies, including electronic technologies and the certification processes for electronic voting and other technologies, without requiring election observation missions to enter into confidentiality or other nondisclosure agreements concerning

[26] German Federal Constitutional Court judgment on the use of electronic voting machines, 3 March 2009. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html.

[27] DoP, Para 14, "Political contestants (parties, candidates and supporters of positions on referenda) have vested interests in the electoral process through their rights to be elected and to participate directly in government. They therefore should be allowed to monitor all processes related to elections and observe procedures, including among other things the functioning of electronic and other electoral technologies inside polling stations, counting centres and other electoral facilities, as well as the transport of ballots and other sensitive materials."

[28] Explanatory Memorandum to Council of Europe Recommendation CM/Rec(2017)5. Paragraph 98. https://rm.coe.int/168071bc84

technologies or election processes, and recognises that international election observation missions may not certify technologies as acceptable…"[29]

Finally, in the context of transparency, the adoption of an open electoral data approach is a good practice that would ensure a higher level of transparency and access to all stakeholders, greatly fortifying the trust in the electoral process.

Accountability

Elections are the primary means by which voters hold those elected to office accountable. There must also be accountability within an election process if it is to be genuine and reflect the will of the people.

EMBs are the focus of the principle of accountability for the electoral process, including for e-ICT systems. However, accountability extends also to vendors, certification bodies and others involved in procurement, management and implementation. Election officials should be responsible for the overall conduct of elections, including oversight of e-ICTs. If e-ICTs involve technology supplied by private vendors, the roles and responsibilities of these vendors must be clearly defined, as well as adequate mechanisms for their management and oversight. Similarly, certification agencies and other bodies must be held strictly accountable in order to ensure they fulfil their respective responsibilities.

Applying the principle of accountability to elections using e-ICT systems can be challenging. First, determining the consequences of some actions taken by officials may need to face a lack of transparency as they may not be visible (since they take place within a machine) or well understood, therefore establishing the accountability becomes more complicated unless the machine keeps accurate records of its use. Second, many aspects of implementing e-ICT systems require EMBs to have highly skilled personnel and institutional awareness of ICT issues. Third, given these considerations and the technical nature of the process, it is common for commercial vendors to assist the EMB, in some cases coming close to assuming some EMB responsibilities, which may call into question the principle that the EMB is solely accountable for the entire process.

EMBs should strive to ensure their own accountability. It is particularly important that each action taken is properly recorded by the system and is verifiable. The process of procuring and adopting new e-ICT solutions should be inclusive and transparent. This is especially necessary in a situation where new technologies are implemented that may not be broadly understood by the public or electoral contestants. EMBs can also allow political parties, election observers and the media to attend meetings where policies are being formulated, particularly in regard to the introduction and use of new technologies. Post-election audits and "lessons learned" exercises also help to foster ownership of the process by electoral stakeholders.

EMBs should remain in control of the relationship with the vendor and ensure the relationship does not violate their own sovereignty over the electoral process.

[29] DoP, Para 12(b).

This applies especially to the processing of data that is collected and stored, which belongs to the state and is subject to the country's laws and requirements as well as to the jurisdiction of the national judicial system. In an election where certain stages of the process are contracted to third parties, the EMB still retains overall responsibility. The role of the vendor must be clearly defined so the EMB retains control of the process at all times; more specifically, the EMB should remain the data controller, determining the purpose and means of processing of personal data. Vendor lock-in situations – where the EMB cannot easily change providers because not all essential information about the system is available for efficient takeover by an alternative provider – should be avoided.[30] It is the responsibility of the election officials to ensure the process meets deadlines and legal requirements, and to liaise closely with vendors to make sure these criteria are met.

Digital Security

The increasing use of ICT systems worldwide and their vulnerability to malicious manipulation from both national and foreign agents has made cybersecurity one of the crucial factors to preserve public trust, especially in the context of e-ICT. Therefore, in recent years, there has been an increase of awareness and action to make e-ICT systems more secure and less susceptible to alleged or actual manipulation.

Protecting the computer-based election hardware and software is essential for election integrity. There is a vast and decentralised ecosystem of technologies that support elections, including online voter registration systems, electronic voter identification systems in the polling stations, electronic voting and counting, results tabulation systems and auditing systems. All of these technologies are susceptible to digital attacks as well as internal errors, both of which can erode voter confidence and impact the integrity of elections.[31]

The UN Secretary-General's High-level Panel on Digital Cooperation has suggested that digital trust, security and stability be the main areas for multilateral cooperation in order to 'shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible use of technology, and propose priorities for action.' It has called for a multi-stakeholder Global Commitment on Digital Trust and Security to bolster existing efforts[32] in this area. Another key area of action is to deepen cooperation and information sharing among national Computer Emergency Response Teams

[30] European Commission decisions in a procurement context: Against lock-in: building open ICT systems by making better use of standards in public procurement, COM (2013) 455 final, p.4.; "Sharing and re-using" clauses for contracts, Contractual Clauses for Service Procurement, p.22. ; Guide for the procurement of standards-based ICT — Elements of Good Practice SWD (2013)224 final, p.33.Guideline on public procurement of open source software (2010), p.42, 56. ; Guide for the procurement of standards-based ICT — Elements of Good Practice SWD (2013)224 final, p.33.

[31] 'Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age', January 2020: https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf

[32] The UN Groups of Governmental Experts (GGE) on Developments in the field of Information and Telecommunication in the context of International Security, set up in 1998, whole proposed eleven voluntary and non-binding norms for member states were welcomed by the UNGA in 2015.

(CERTs). These initiatives not only include member states and regional organisations, but also the private sector.

In this context, a number of initiatives should be noted, both at global and regional level.

In terms of wider cybersecurity and international cooperation around securing electoral integrity, it is worth mentioning the cooperation that has developed around the Paris Call for Trust and Security in Cyberspace initiative,[33] launched in 2018, which specifically calls for a strengthening of capacities to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities[34]. At regional level, the EU Network and Information Systems (NIS) Cooperation Group published in 2018 the "Compendium on Cyber Security of Election Technology"[35]. The Council of Europe's Cybercrime Convention Committee has also produced a brief guidance note[36] on the application of its provisions to election offences. The Commonwealth Guide on Election Cybersecurity[37] describes principles for election cybersecurity as well as specific institutional recommendations that can be adapted by EMBs[38], together with technical guidance that can help with specific challenges. Similar recommendations can also be found in IFES' 2018 Holistic Exposure and Adaptation Testing (HEAT) Process.[39] Similarly, recognising the need for inter-agency cooperation, the International Institute for Democracy and Electoral Assistance (IDEA) published "Cybersecurity in Elections – models of interagency collaboration"[40] in 2019.

Stakeholder Responsibilities

This chapter focuses on the specific responsibilities that stakeholders, both national and international, have for the implementation of e-ICTs in the electoral process. Guidance on the different stages of implementation of e-ICTs is available in publications[41] from various international organisations.

---

[33] The Paris call was launched in 2018 and joined by 65 countries and 334 companies, amongst which the main global tech companies and 138 universities and NGOs. Many leading technology powers such as the US, Russia, China, Israel and India have not yet joined the initiative.
https://pariscall.international/en/principles

[34] An interesting initiative addressing the vulnerability to cyberattacks of political parties and candidates was promoted by NDI and IRI which, together with the Harvard Belfer Centre and their project Defending Digital Democracy, have produced practical "playbooks" for specific cases
https://www.belfercenter.org/D3P#!playbooks

[35] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645

[36] Aspects of election interference by means of computer systems covered by the Budapest Convention, adopted 8 July 2019: https://rm.coe.int/t-cy-2019-4-guidance-note-election-interference/1680965e23

[37] https://thecommonwealth.org/sites/default/files/inline/Cybersecurity_for_Elections_PDF_0.pdf

[38] Similar recommendations can also be found in IFES: 'Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies'.
https://www.ifes.org/publications/cybersecurity-elections

[39] https://www.ifes.org/publications/cybersecurity-elections

[40] https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

[41] ACE Project, 'Elections and technology'. https://aceproject.org/ace-en/topics/et/onePage
Council of Europe, 'recommendation (2017)5 on standards for e-voting'.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f
European Commission, 'Guide for the procurement of standards-based ICT — Elements of Good Practice'.
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2326

The Election Management Body (EMB)

The EMB has responsibility and accountability for the whole electoral process, including all aspects of the adoption, procurement, deployment and use of e-ICT solutions. Together with the national parliament, the EMB should be the body responsible for facilitating the reflection and discussion that might lead to the adoption of e-ICTs by setting up broad consultations with political actors and civil society in order to reach a fact-based decision that takes into account the widest possible spectrum of opinions.

It is important to note, if implemented according to good practice, the process of adoption may be quite lengthy; therefore, the EMB should give adequate consideration to its timing in relation to the electoral cycle. A rushed introduction will inevitably result in some stages of the process not being fully implemented, with possible negative impact on the quality of the result and on the trust stakeholders will have in the e-ICT. The timetable for introduction of e-ICTs should include adequate time for the conduct of a feasibility study and for pilots and testing of the new e-ICT. This should also be supported by timely and adequate funding from the national authorities once a project is adopted.

Throughout the process, another EMB key task is to ensure the transparency of the process, an important factor for enhancing the trust of stakeholders, this includes both giving meaningful access to relevant documentation to stakeholders and observers and to keep the public informed through voter information programmes.

Where the integrity of a critical infrastructure[42] is at stake, stringent requirements and control procedures should be applied to the implementation of e-ICTs, with particular regard to their integrity and security. In cases where, for various reasons, the EMB cannot summon the necessary technical expertise to lead throughout this process, expert support should be provided either by national

---

EU-UNDP Joint task force, 'Procurement Aspects of Introducing ICTs solutions in Electoral Processes: The Specific Case of Voter Registration' (2010) http://aceproject.org/ero-en/misc/procurement-aspects-of-introducing-icts-solutions;
IDEA, 'Introducing electronic voting: essential considerations'.
https://www.idea.int/es/publications/catalogue/introducing-electronic-voting-essential-considerations
IDEA, 'Introducing Biometric Technology in Elections', (2017),
https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf
IFES, 'Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies' (2011),
https://www.ifes.org/sites/default/files/electronic_voting_and_counting_tech_goldsmith_0.pdf
IFES and NDI, 'Implementing and Overseeing Electronic Voting and Counting Technologies' (2013),
https://www.ifes.org/sites/default/files/implementing_and_overseeing_electronic_voting_and_counting_technologies_0.pdf

[42] Critical infrastructure refers to systems and assets for which "incapacity or destruction...would have a debilitating impact on security, national economic security, national public health or safety, or any combination." The US Department of Homeland Security designated the systems and assets used to administer elections as a critical infrastructure subsector in 2017. This includes physical locations (storage facilities, polling places, and locations where votes are tabulated) and technology infrastructure (voter registration databases, voting systems, and other technology used to manage elections and to report and validate results). It does not include infrastructure related to political campaigns. In the EU, the Agency for Cybersecurity ENISA proposed the same designation in the context of the 2019 European Parliament elections.

actors or external sources and commercial providers should be required to exercise extreme due diligence in their practices.

With technical support from specialised agencies (such as cybersecurity and data protection agencies) and other external expert support, the EMB should lead the crucially important phase of defining the technical specifications of the e-ICT solutions that the country has decided to adopt, and make sure that the fundamental principles for elections described in the first part of this document are ensure by the proposed e-ICT. If the necessary expertise is available, it should also cover the phase of the feasibility study, piloting, testing, certification of the system and subsequent regular audits, otherwise such expertise will need to be identified from abroad. In situations where this cannot be developed internally and needs to be outsourced, the EMB has also overall responsibility for the key phase of tendering and procurement for the e-ICT, acting under the national framework for public procurement (which should be based on transparency, competition and objective criteria in decision-making) and eventual anti-corruption frameworks connected to procurement.

Procurement should be managed with consideration for the electoral calendar, otherwise there is a risk of rushed tenders awarded under non-transparent decisions and with key issues not being included in contracts. Procurement done in haste and with a direct award (sole source contract) should normally raise red flags for national watchdogs, and do not contribute to public trust in the systems adopted. When the EMB cannot rely on professional technical expertise, blind trust is sometimes placed in commercial providers. Such practices have important negative implications on the overall trust of stakeholders in e-ICTs and might also lead to a solution that does not work as intended, potentially compromising the integrity and credibility of the whole electoral process.

Key international texts on procurement[43] underline the importance of procurement transparency and of public information to strengthen the confidence of stakeholders in the process. For national stakeholders, having unimpeded access to relevant documentation is a critical precondition for playing their roles in a meaningful way. International observers can also play an important role by assessing if this right has been adequately granted to national stakeholders, as well as conducting analysis about the system itself.

After the tender for an e-ICT solution is awarded, the EMB should continue to exercise its responsibility and follow-up on the execution of the contract with the vendor. Here the EMB should supervise the implementation, ensuring that the vendor is not in a position to take any action affecting the functionality of the equipment without EMB authorisation. For the EMB it is important that the

[43] 'OECD Principles for Integrity in Public Procurement' identifies the two key principles underpinning procurement transparency: a) Provide an adequate degree of transparency in the entire procurement cycle in order to promote fair and equitable treatment for potential suppliers, b) Maximise transparency in competitive tendering and take precautionary measures to enhance integrity, in particular for exceptions to competitive tendering. https://www.oecd.org/gov/ethics/48994520.pdf
Art. 9 and 10 of the 'UN Convention against corruption' also outline important transparency and public information aspects of a procurement process.
https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

procurement process leads to contractual requirements that include firm deadlines for delivery corresponding to the electoral calendar, and adequate time to conduct audits of the equipment and remedy any deficiencies in vendor performance, as well as sufficient penalties to deter non-performance.

EMBs should also make sure that the e-ICT solutions are tested and certified by an independent authority before being approved for use. Audits can be conducted at regular intervals to verify that the equipment in use is the same as that which was certified. It is important to underline also that the certification of e-ICT solutions does not fall within the remit of international observers.

Finally, while EMBs have a special responsibility to balance the pros and cons of introducing e-ICTs, it is critical that the electoral process continues to belong to citizens, upon whose will the authority of government is based.

While the EMB may be held accountable by a variety of institutions and stakeholders, the accountability of the EMB should be reinforced by a strong and independent judiciary, which usually plays a key role in adjudicating disputes at least in the last instance, including those related to e-ICTs. One common accountability challenge in the context of digital systems, including e-ICTs, is the lack of mechanisms for collective redress, that would allow organisations to bring complaints on behalf of an unspecified number of people who have negatively been affected. In the specific case of the EMB, the role of the judiciary can also be complemented by legal requirements for public information on complaints made to EMBs, adding an extra layer of transparency to its work.

Other national stakeholders

National stakeholders, political parties, civil society (including election observers) and the media have an important role to play in early deliberations over the adoption of e-ICTs by participating in initial discussions. Following this, all electoral stakeholders have a crucial responsibility to hold EMBs accountable by monitoring their activities and bringing any violations to the attention of the judiciary and the public. Because of the technical nature of e-ICT systems, stakeholders may need to develop specific skills to give meaningful input into deliberations, and especially media have a responsibility for developing appropriate understanding of systems in use as far as needed for accurate reporting. Understanding the systems enables national stakeholders to detect violations and collect the necessary evidence to file a complaint.

In this context, it is also vital that political parties engage proactively and responsibly in the consideration and possible adoption of e-ICTs and proactively inform supporters on what a new system is meant to bring to the election. If all contestants are equally informed and agree on the technical solution and there is transparency in the overall process, there should be no grounds for unspecified allegations of electoral manipulation connected to an e-ICT system.

As mentioned above, expertise from either specialised national agencies (cybersecurity and data protection agencies) or other external expert support can

be put at the disposal of the EMB during the more technical phases to make sure the common goal of procuring the best solution possible is achieved.

E-ICT Manufacturers and Vendors

The concerns of manufacturers and vendors of election technology are different from those of election officials. Their primary aim is to make a profit by delivering on the contract concluded with the EMB.

Manufacturers and vendors are duty-bound to respect codes of business practices[44] or other regulatory frameworks that apply. In addition, given the critical importance of electoral systems in the democratic life of a country, more stringent requirements of due diligence[45] should be applied**.** Given that due diligence should be commensurate with risk and appropriate to the circumstances and context of a specific enterprise, the degree of due diligence exercised in designing an e-ICT system should be similar to that used to ensure the integrity of a critical infrastructure. This has clear implications also for the conceptualisation, design and testing phases of new ICT products – as well as the underlying datasets and algorithms that support them. This should all be subject to proactive human rights due diligence.[46]

As the UN Guiding Principles on Business and Human Rights (UNGPs) note: "human rights due diligence should be initiated as early as possible in the development of a new activity or relationship, given that human rights risks can be increased or mitigated already at the stage of structuring contracts or other agreements." Human rights due diligence can be included within broader enterprise risk-management systems provided it goes beyond simply identifying and managing material risks to the company itself to include risks to rights-holders. The guidelines also suggest that businesses "treat the risk of causing or contributing to human rights abuses as a legal compliance issue wherever they operate."[47] On the subject of corporate due diligence in the area of human rights, work is progressing to go beyond the UNGPs.[48] In 2014, the EU published an ICT

---

[44] For instance, the OECD published in 2018 guidelines for responsible business conduct, aiming to help enterprises avoid and address adverse impacts related to workers, human rights, the environment, bribery, consumers and corporate governance that may be associated with their operations, supply chains and other business relationships. https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf

[45] The concept of human rights due diligence is a critical part of fulfilling the "corporate responsibility to respect" as defined in the UNGPs. Human rights due diligence refers to the processes that all business enterprises should undertake to identify, prevent, mitigate and account for how they address potential and actual impacts on human rights caused by or contributed to through their own activities, or directly linked to their operations, products or services by their business relationships. is being also developed in the context of drafting of the UN Treaty on Business and Human Rights, https://www.business-humanrights.org/en/un-treaty-on-business-human-rights-negotiations-day-1-the-round-of-discussions-kicks-off-with-an-improved-draft.

[46] OHCHR B-Tech project Overview and scope. https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Project_revised_scoping_final.pdf

[47] UN Guiding Principles on Business and Human Rights, point 23(c), p.25.

[48] In the context of the UN Road map for digital cooperation, the UN High-level panel is conducting work on how the international community can work together to optimise the use of digital technologies and mitigate the risks in the framework of achieving the Sustainable Development Goals. More specifically on digital technologies and human rights, the Office of the UN High Commissioner for Human Rights is to develop

sector guide on implementing the guiding principles.[49] A number of governments have recently either introduced, or have announced their intention to consider, the introduction of legislative regimes to encourage or require companies and corporate groups to carry out mandatory human rights' due diligence.[50]

Some fundamental principles can be embedded in the design of a system, making it even more likely they will be respected when the system is operating. It is important, then, that commercial providers also view these principles as their ultimate goal when considering the production of new e-ICT systems.

International Donors and Technical Assistance Providers

International donors and technical assistance providers also bear some responsibility for the proper implementation of e-ICTs. Donors occasionally fund e-ICT systems as part of their democracy support and electoral assistance programmes and should therefore ensure that the introduction of new technologies respects democratic principles and promotes human rights. Their foremost responsibility is to the beneficiaries; thus it becomes even more important to support EMBs in situations where they lack the necessary skills and knowledge to properly evaluate and decide on the introduction of e-ICT solutions.

The first duty of donors should be to help bridge the skills gap, and not leave EMBs to decide in the dark. In such a situation, important questions should be answered about the sustainability of the project, as the EMB might not have the necessary capacity for overseeing the implementation of the solution, as well as its ongoing management and maintenance. Electoral assistance providers should impart expertise to accompany the EMB in its decision-making process, as well as in the testing and introduction of e-ICTs and the training of national stakeholders to allow them to play their role in ensuring the accountability of the EMB during the process.

In case donors decide to support an EMB in the adoption of e-ICT solutions, they should ensure that the adoption is based on inclusive analysis to identify the most effective technology to respond to jointly identified challenges and the given socio-economic context. Supporting a thorough feasibility assessment, including a risk, cost and sustainability assessment, in an inclusive process before any decision to proceed should be the standard practice. The procurement of technological solutions should be done according to national laws and international standards, in full transparency and should be followed by the

---

system-wide guidance on human rights due diligence and impact assessments in the use of new technologies under the B-Tech Project started in 2019.
https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf;
https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx .

[49] The EU has also published sector-specific guidance to ICT firms on how to implement the UNGPs.
https://op.europa.eu/en/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b/language-en.

[50] There appears to be momentum behind these proposals in some European Union and European Economic Area member states and also within EU institutions. 'UN Human Rights "Issues Paper" on legislative proposals for mandatory human rights due diligence by companies'
https://www.ohchr.org/Documents/Issues/Business/MandatoryHR_Due_Diligence_Issues_Paper.pdf

adoption and testing of the e-ICT system as well as its gradual introduction, training of stakeholders and effective voter education[51].

Ultimately the decision to adopt an e-ICT solution remains a sovereign decision for the EMB and national stakeholders. At the same time, donors should consider the issues of need, sustainability and effectiveness of any proposed e-ICT system and only support solutions that are compatible with fundamental principles for democratic elections, due diligence and ethical design.[52] Such considerations should provide guarantees in terms of functionality, security and the EMB's authority over the electoral process.

Consideration should also be given to potential compatibility with initiatives aimed at ensuring transparency of governance systems, codes of good practice and other initiatives that strive to promote transparency, such as the Open Data initiative.[53] This initiative has also been adapted to cater for elections through the Open Election Data Initiative,[54] launched by NDI, which sets out principles and provides training modules for EMBs, election observers and others. Such efforts should help make the next generation of e-ICTs more likely to guarantee the fundamental principles for democratic elections. Open data is crucial to electoral integrity in the digital era and is essential to public trust in elections. It can help improve the flow of information within and among governments and make government decisions and processes more transparent. Increased transparency promotes accountability and good governance, enhances public debate, helps combat corruption and ultimately enhances the credibility of the electoral process.

[51] In cases where a specific donor, for instance the EU, finances the procurement, additional specific considerations related to the donor should be considered, for example that EU standards for electronic identity, cybersecurity and data protection be included in the procurement.
[52] G. van Oortmerssen, "Ethics and ICT: Beyond design," 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, 2014, pp. 1-6, doi: 10.1109/ETHICS.2014.6893400.
[53] The six charter principles were developed in 2015 by governments, civil society, and experts around the world to represent a globally agreed set of aspirational norms for how to publish data. https://opendatacharter.net/principles/
[54] https://openelectiondata.net/en/

Summary

The following are a set of non-exhaustive conditions necessary for e-ICTs to contribute to the integrity of the electoral process and public confidence in it:

General principles:

a) E-ICT systems should respect the key principles for democratic elections, including the integrity, secrecy, universality and equality of the vote, transparency, accountability, digital security and public confidence (trust). Fundamental principles for democratic elections should be considered and applied in the design of an e-ICT system, making it more likely the principles will be respected when the system is operating.
b) A legal and operational framework should complement e-ICT systems, providing a solid base for the fundamental principles for democratic elections to be respected, including processes that provide for the transparency and accountability needed for their adoption and use, as well as for their security.
c) The introduction and implementation of e-ICT systems should take an inclusive approach, involving a broad range of stakeholders throughout the process, to promote transparency and public confidence.
d) The adoption of e-ICTs should be based on the most inclusive analysis possible with national stakeholders, to identify the most effective solution to respond to jointly identified challenges and the given socio-economic context. It should be preceded by a thorough feasibility assessment, including risk, cost and sustainability assessments.
e) The procurement of e-ICTs should be done according to national laws and international standards, in full transparency and it should be followed by the adoption and testing of the e-ICT system as well as its gradual introduction, training of stakeholders and effective voter education.
f) Individual and universal verifiability are key elements of maintaining public trust and confidence when introducing e-ICTs. Increasingly, the use of voter verified paper audit trails (VVPAT) for electronic voting machines is considered to be an emerging good practice, one that is increasingly recommended by election observers and technical assistance providers alike, along with having appropriate audit procedures in place (e.g., risk limiting audits).
g) Election observation is a key aspect of transparency and observers should have access to all documents and have the opportunity to observe all phases of the election process.

Election Management Bodies (EMB):

h) EMBs have responsibility and accountability for the whole electoral process, including all aspects of the process of adoption, procurement and functioning of e-ICT solutions.
i) EMBs should provide for a broad consultative process on whether to introduce e-ICTs that is inclusive of political and civil society actors and takes into account the widest possible spectrum of opinions.
j) If implemented according to good practice, the process of adopting an e-ICT may be quite lengthy; therefore the EMB should give adequate consideration to its timing in relation to the electoral cycle. A rushed

implementation will inevitably result in some parts of the process not being fully implemented, with a negative impact on the quality of the process and on the level of trust that stakeholders will have in the e-ICT.

k) The EMB and Parliament should ensure that e-ICTs are introduced under the condition that adequate time and funding are available for proper deliberation and implementation in line with international good practice. Time needs to be allowed for public consultation, needs assessment, feasibility study, procurement, legislative changes, piloting, certification and testing processes to be carried out, as well as parliamentary oversight and legal accountability. Often this requires more than one election cycle.
l) A critical EMB task is to ensure the transparency of the process at all stages, a key factor for enhancing the trust of stakeholders. This includes both giving meaningful access to relevant documentation to stakeholders and observers and keeping the public informed through voter information programmes.
m) It is the EMB's responsibility to ensure the e-ICT implementation process meets deadlines and legal requirements, and to liaise closely with vendors to ensure these criteria are met.
n) A certification/auditing process of e-ICT systems should be led by independent experts or institutions, but national actors, the EMB first and foremost, should maintain the overall responsibility for the process. EMBs should also promote transparency by providing information on testing and certification undergone by e-ICT systems and by allowing meaningful observation of these processes.
o) Sovereignty principles require that data collected by the e-ICT system belong to the EMB, comply with national laws and regulations on transparency and privacy, and be subject to the jurisdiction of national courts.
p) EMBs must ensure that electoral data is open to all citizens to understand, evaluate and ultimately accept the credibility of the election. Data collected by the e-ICT should belong to the EMB, must comply with national laws and regulations for transparency and privacy and be subject to the national courts' jurisdiction.

Other national stakeholders:

q) National stakeholders, political parties, civil society (including election observers) and the media should play an important role in inclusive and broad discussions over the adoption of e-ICT.
r) They should also act as watchdogs and scrutinize the process of tendering, testing, installation and use of the e-ICT system.

E-ICT manufacturers and vendors:

s) Given the critical importance of elections in the democratic life of a country, manufacturers and vendors of e-ICT systems should adhere to stringent requirements of corporate accountability and responsibility and human rights due diligence and equally stringent requirements for dependability and performance.

Donors and electoral assistance providers:

t) Donors should ensure that if they support the introduction of technology in elections, that it is based on independent and inclusive analysis to identify the most effective technology to respond to jointly identified challenges and the given socio-economic context. Supporting a thorough feasibility assessment, including risk, cost and sustainability assessments in an inclusive process before any decision to proceed should be the standard practice.