NDI

NATIONAL
DEMOCRATIC
INSTITUTE

Monitoring
Electoral Electronic Technologies:
A Model Checklist

2024

Table of Contents

Introduction

The increased presence of electronic technologies in our daily lives has brought considerable and concrete benefits. We can communicate with friends, family, and colleagues seamlessly through email, social media, or messenger apps, send or receive money on our mobile devices, have faster and easier access to information, and conduct our work more efficiently and with fewer mistakes. While the use of new technologies in the administration of elections is not new, in recent years there have been growing calls for electronic technologies to be incorporated into critical election processes - such as voter registration, polling day procedures and tabulation - to make them more efficient, user friendly and error free, ultimately increasing public trust.

However, it is also important to recognize that any changes to election procedures have the potential of introducing additional challenges to electoral integrity. Technology solutions that are the product of opaque processes result in less transparency or are prone to failures could result in less, not more, public trust in the technology and the electoral process as a whole. The systemic failure of some technologies, such as the ones used to identify voters, count and aggregate votes, or transmit results, could cast doubt on the credibility of the election.

Recognizing both these benefits and threats, the community of organizations endorsing the Declaration of Principles for International Election Observation identified a set of principles and guidelines for the adoption of new electoral information and communication technologies (e-ICTs) in election administration.[1] Based on these principles, summarized in the table below, NDI has developed the current checklist as a practical tool for citizen and international observers to adapt to their own context as they seek to determine whether the procurement, design and implementation of electoral electronic technologies are conducive to the inclusion, transparency and accountability of the election process.

[1] General principles and guidelines related to ICT and elections: A DoP technical document. Available at www.ndi.org/eet.

Principles for the Adoption of e-ICTs

Universal Suffrage	All eligible adult citizens must have the opportunity to vote, including those not familiar with technology.
Transparency	Inclusive and continuous engagement with stakeholders – from inception to implementation and use – as well as access to all election processes and relevant data, is essential for building trust and avoiding incorrect perceptions.
Equality of the Vote	No voter can cast more votes than another.
Integrity of the vote	Votes should be recorded, counted and tabulated in accordance with ballots cast by voters at the polling station. Systems must allow for meaningful and timely verification of ballots without compromising the secrecy of the vote.
Secrecy of the Vote	Voters must not be able to prove to anyone how they voted, and the system itself must not allow identification of a voter's vote.
Digital Security	To preserve the integrity of the election and avoid the erosion of public trust, e-ICTs must be designed, implemented and tested to reduce their vulnerability to internal errors and malicious manipulation by national or foreign actors.

How to Use This Guide

This document includes a list of questions that can guide observers' assessment of new technologies being adopted. In some cases, the questions can be answered through direct observation. In others, they will require observers to consult election officials or technology vendors, partner with technology or anti-corruption experts, or review technical specifications. The document, however, does not assume or require observers to directly assess the code, hardware or any other technical element.

For ease of use, the checklist is organized to include a set of cross-cutting issues that apply across multiple technologies, followed by issues that are specific to a given type of technology. Questions are further organized by the period when they apply, including preparations, the performance of the technology when in use, opportunities for recourse as applicable, and a comprehensive review following the election. For each section, the checklist includes general questions that seek to assess whether the adoption of any new technology is consistent with the principles mentioned earlier.

When using this guide, observers will want to consider both new election technologies under consideration and their country's track record of past technology adoption. This will provide observers a greater understanding of the strengths and weaknesses of past processes and can yield additional information on aspects of the adoption process that might warrant special attention while monitoring. Similarly, observers may need to prioritize certain phases of the process depending on the context and type and nature of election technologies being introduced. Observers should consider the likely impact that a particular technology might have and at what phase that it might be open to the greatest opportunity for abuse and manipulation, at the same time identifying what is observable through direct or indirect means.

Observer engagement and oversight of the introduction of new technologies will ideally occur during the initial concept and proposal phases, well ahead of their adoption and implementation. However, this is not always possible due to numerous factors, including a lack of transparency or inclusiveness of the process, as well as observer funding and resource limitations. If observers are unable to engage throughout the process, it is critically important for groups to understand to what degree national laws and international standards are being met.

Refining Lines of Inquiry

The questions listed below are general and can be used by civic organizations to guide discussions on what to observe in their country context. Election observers can use these general questions to identify observable indicators that they can use in their data collection tools, such as checklists for direct observation or open election data analysis.[2]

For example, when thinking about training for election officials, the checklist below guides citizen observers to ask, "Are training materials accessible to all trainees, including in terms of language and literacy?" However, in a specific country context, observers would want to think about accessibility in different ways. This might include:

- Online vs. offline training;
- Physical location of the training;
- Capacity to use certain types of technology;

[2] For example, the Open Election Data Initiative (OEDI) provides additional information on how observers can analyze and assess open data on key aspects of the election process. OEDI is available at www.openelectiondata.net.

- Specific languages spoken by marginalized communities; and
- Ability to read and write in a particular language.

Section I: Cross-Cutting Issues for All Technologies

Identifying the need for a technology solution

The idea of adopting e-ICTs can be introduced by a variety of actors — including ruling or opposition parties, citizen election observers or other activists, election commissions, vendors, and others — for a variety of reasons. Actors may push for the adoption of e-ICTs to make aspects of the election process more transparent or efficient. For example, countries concerned with rendering the voting process more accessible for persons with disabilities might consider electronic voting. Countries that have experienced issues with multiple voting might look to biometric voter registration and identification. Where there are tensions around the collation and results aggregation process, countries might consider electronic results transmission technologies.

However, there can also be negative incentives for introducing new technologies. Observers should consider the environment and incentive structures under which the decision makers put forward the idea of adopting e-ICTs, and whether they have identified a clear **need for a technological solution**.[3]

Model Questions

- What gaps are being filled with the technological solution, if any?
- In the past, have nonpartisan, independent election observers or other experts identified the need for a technological solution? Who else has advocated for one?
- Did the EMB carry out a *needs* assessment prior to making the decision to adopt a technological solution? Were the findings of this assessment shared with the public? Were assessment recommendations implemented?
- Who proposed the specific technological solution? Was there any undue pressure to use a particular platform or solution?
- Who was consulted in the decision to adopt the technology? How open were the consultations?

[3] For more information on the decision-making process, see "Making a Decision on E-voting or E-counting" in *Implementing and Overseeing Electronic Voting and Counting Technologies,* authored by NDI and IFES (2013): https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies.

- Did key stakeholders raise any political, technical, or other concerns? If so, were those concerns sufficiently addressed? Did the EMB carry out a *feasibility* and *cost* assessment prior to making the decision to adopt a technological solution? Were the findings of these assessments shared with the public? Were assessment recommendations addressed?

Legal framework

As the decision to adopt electronic technologies for critical election processes is being made, it might be useful to review the **legal framework**, including regulations developed by EMBs and other administrative authorities, to ensure that there are no provisions that would prevent the adoption of the recommended technology, or lead to legal complaints about its use. At the same time, legislation authorizing the use of e-ICTs for critical aspects of the election process should address questions regarding authority to adopt new e-ICT solutions; requirements for testing and certification; analog redundancies as backups for electronic technology and audits; chain of custody in results management; resolving inconsistencies and determining primacy of electronic and manual information sources; and, perhaps most importantly, provide a framework for legal recourse for citizens or stakeholders seeking redress in cases when the use of e-ICTs has affected their civil and political rights.

Model Questions

- Does the legal framework indicate who has the authority to decide to adopt e-ICTs and what processes they must follow to make this decision?
- Are there processes outlined for verifying the integrity of the technologies through testing? Is there a requirement for certification?
- If the legal framework required updates related to the adoption of electronic election technologies, were there opportunities for inclusive consultations with stakeholders?
- Does the legal framework outline requirements for a paper audit trail demonstrating what actions were taken using electronic technologies?
- Does the legal framework indicate whether there will be a “manual” backup or redundancy for technology, including specifying which version will serve as the official record, in case of discrepancies?
- Does the legal framework outline the chain of custody for information gathered using e-ICTs, such as the transmission and verification of data on voter registration data, voter identification, and results?
- Does the legal framework outline provisions on data privacy as well as transparency and openness of election data as it relates to election technology?

- Audits:
    - Does the legal framework include provisions for recounts, in case of a challenge?
    - Does the legal framework include provisions for auditing a sample of the work done using technology for any phase of the process? (Recount a sample, audit a sample of voter registration records or voter identification records, etc.)
    - Does the legal framework explain the conditions under which an audit will take place? Does it provide for independent audits to take place?
    - What are the requirements to challenge the use of technology at any phase of the process? Who has the legal standing to do so?
- Does the legal framework guarantee unfettered access to all stages of adoption, implementation, and review processes for e-ICTs to political candidates and their representatives, representatives of ballot initiatives, and independent election observers?

Procurement

Like any election material an EMB will acquire, procuring new technology must follow a clear **procurement process**. Many countries apply general regulations for public procurement to the electoral process, though EMBs may have particular rules in place for certain types of materials or procurements over a certain budget amount. Transparency is key when assessing the credibility of a procurement process for new election technology.[4] Equally important, procurement decisions should take into consideration not only the cost of implementing the selected technology for the next election, but also any materials, labor and service costs associated with its maintenance and upkeep for use in future elections. Similarly, decision makers should understand whether costs presented in a vendor's bid correspond to the true cost of long-term implementation, or if it reflects any discounts or subsidies that would not be available in the future.

Model Questions

- Does the legal framework and/or EMB policy set out clear guidelines or regulations for the procurement process?
    - Did the procurement of the new technology follow that process?

[4] For more resources on evaluating procurement processes, see the Open Contracting Partnership (https://www.open-contracting.org/) and https://www.ndi.org/eet.

    - If not, what was the justification for deviating from the established process?
- Was the procurement conducted with enough time to allow full compliance with legal requirements, and to reasonably design, implement and test the selected technological solution?
- Was the bidding process open to a wide range of potential vendors?
- Were the requirements for the bid reasonable, so that any reputable vendor could reasonably meet the requirements, or was the process tailored to one vendor?
- What process was followed for reviewing and scoring the bids? Was this process open and transparent?
- Were there any potential (perceived or real) conflicts of interest in the procurement process?
- Is documentation from the procurement process available to the public, including bids as well as notes from the evaluation of bids and the decision-making process?
- Does the procurement set clear requirements to ensure data ownership and data privacy?
- Are there requirements in the procurement process – including in the request for proposals, bid evaluation criteria, or other components – to ensure adherence to internationally-recognized principles for the adoption of e-ICTs? (see p. *Principles for the Adoption of e-ICTs* table for more information)
- Do cost applications reflect the long-term cost of maintaining and updating the technology and applying it in future elections? Are there any discounts, subsidies or other hidden costs that would increase the cost of implementation in the future?
- Was the final selection justified based on the appropriateness of the technical solution, the approach to quality assurance and transparency, and sustainability, including the cost of long-term adoption?

Testing

Elections are high stakes, and technology failures or mishaps can create serious challenges to citizen trust in the electoral process. Once procured, all technology must be tested to ensure that it is ready to use. Observers should have access to this testing process, and should consider the scale of the test as well as the degree to which it mimics real conditions, and how any challenges will be addressed.

Model Questions

- Was testing completed with ample time available for any difficulties to be addressed prior to the technology being used in the electoral process?

- How large-scale was the test? Was there a pilot initiative to use the technology in a lower-stakes process, such as a by-election, primary election, or other opportunity?
- Were conditions for the test similar to when the technology will be used in the pre-election process, on election day, or after the election? This may include:
    - Environmental factors: Weather, light, electricity
    - Infrastructure: Access to electricity and internet, road conditions, transportation, shelter from weather
    - Diversity of the population: Age, language, geography, physical features
    - Stress testing: Load testing, battery life
    - Time of day: When information is transmitted, votes counted or the voters' list printed
- Did the technology behave as expected regardless of the conditions under which it was tested? Did it produce the same result consistently when presented with the same input (e.g. a fingerprint, or a bubble filled in a ballot)?
- Did the EMB publicly communicate about any challenges that arose during the test and how they will be addressed?
- Were there multiple phases of the testing process, and were tests repeated?
- Were all aspects of the testing process open to election observers?

Certification

In addition to testing technology on their own, EMBs seeking to follow best practices may also have an independent body certify the technology and its readiness for use in the electoral process. This certification requires specialized technical expertise that observers are not expected to have. However, the certification process should be inclusive and transparent, and allow contestants, observers and other actors to engage in the process and have access to any findings and recommendations. When looking at the certification process, observers should consider who the body that is conducting the certification is, how rigorous their testing is, and how their work is publicized.

Model Questions

- Who is engaged in choosing the certifying body and what process do they follow for selection?
- Who is the certifying body, and what is their prior experience certifying this type of technology in terms of readiness for use?
- What process does the certifying body follow? Do they conduct their own tests, or rely solely on reports from the EMB?

- Is there sufficient space for key stakeholders to engage in aspects of the certification process, from selection of the certifying body, to defining their terms of reference, to following their progress, to accessing findings and recommendations?
- Is the work of the certifying body public, or is there documentation available to the public?
- Has the EMB publicized the certification process to stakeholders and the public?

Inclusive Design and Development

In choosing a technological solution, EMBs will likely be choosing from existing products produced by vendors, but the actual machines and/or software they receive will be customized to fit the local context. In **designing and developing the technology**, the EMB should consider whether it guarantees key election principles, including whether the design of the technology ensures inclusion through accessibility for all voters. This includes addressing barriers to access for voters with disabilities, voters who speak and/or read different languages, voters with varying levels of digital literacy and voters in rural areas with limited digital access.

Model Questions

- Did the EMB engage a wide range of actors who will use the technology during the design process, both as operators and as users, to ensure that the design is inclusive?
- Is the technology accessible to people who are blind, people who are deaf or hard of hearing, and people who use a wheelchair or have other mobility challenges?
- Does the technology lower barriers to access as compared to previously used methods?
- Does the technology allow for use in multiple languages, including both written and audio translations, as applicable?
- If the technology creates additional barriers to full accessibility for all voters, including sociocultural barriers, is there a secure alternative offered to these voters?
- Does the technology require electricity and/or the internet to operate?
    - If so, and if there are areas of the country where there is no electricity and/or internet is not available, does the EMB have a plan for ensuring the electoral process does not become less accessible for people living in these areas?
- Were there specific tests performed to assess the accessibility of the technology for voters facing potential barriers to use?

- Once the decision to adopt a technology is made, have the EMB and/or others carried out sufficient voter education and sensitization campaigns, including those targeting marginalized groups and any potential sociocultural barriers to use?

Staffing and Training

Every election requires a massive **staffing** and **training** component to ensure that those involved in election administration, from the polling station level to the national-level election commission, meet demands for implementation, understand election operations and procedures, and can respond to challenges that may arise. When a new technology is introduced, this component becomes even more important. When looking at staffing and training plans for new technology, observers might consider whether the staff have appropriate skills, training is sufficient and effective, and how this is tested.

Model Questions

- Does the EMB have the appropriate staff to take ownership of the design and implementation of the technology, or are they dependent on external vendors?
- Are there plans and sufficient staffing in place to troubleshoot issues that may arise?
- Does the EMB's training plan include sufficient time to explain the new technology to all who will be involved in operations?
- Did all staff who will operate the technology attend training?
- Are training materials accessible to all trainees, including in terms of language and literacy?
- Were trainings conducted using a standardized curriculum?
- Does the training include a testing mechanism to assess knowledge uptake among the EMB staff?
- Did the trainings include how election officials should provide backups and failsafe options to voters affected by failures in electoral technologies?

Election Dispute Resolution

As technology gets incorporated in different aspects of election administration, its role in **election dispute resolution** is bound to grow. For example, an eligible voter might seek redress after being disenfranchised by a biometric voter identification machine, or an electronic voting machine might need to be included in a vote recount or an audit of election results. To play this role, new electoral electronic technologies must include mechanisms that help verify – or correct – the validity of the information they produce.

Model Questions

- Does the legal framework clearly define how information generated by election technology can or should be used in mounting and resolving electoral disputes? Have steps been taken to ensure that bodies responsible for dispute resolution have the appropriate skills, knowledge, and capacity to adjudicate matters involving election technology?
- Do contestants understand legal recourse available related to the use of technology in elections?
- Does the system produce information that allows stakeholders to mount and/or resolve an electoral challenge, for example through recounts or independent audits?
- Are there paper or manual back ups that could be used if electoral technologies fail?
- Did election officials provide timely redress to citizens affected by failures in electoral technologies, such as biometric voter identification or electronic voting machines?

Audits

In an effort to verify that election technology functioned as intended, EMBs should conduct audits on the performance of the software and hardware. Audits can take place in real time as the system is being used and/or in the post election period to assess any performance, functionality or environmental issues, cost-effectiveness, and to help identify lessons learned. Audits should engage independent experts and ensure key stakeholders are made aware of the audit methodology and outcomes. These exercises can help to build greater confidence in the technology and help to resolve disputes related to the functionality of the technology.

The methodology used to audit each technology solution depends on the system's function and the information it collects or produces. For example, audits could include:

- Independent verifications of voter lists, which could include both computer analysis to identify duplicate entries or other irregularities, and field surveys to ensure the information on the lists match actual citizens.
- Doing a parallel manual count of voter-verified paper audit trails (VVPAT) in a randomly selected sample of polling stations to verify the accuracy of the vote count.
- Verify that a randomly selected sample of paper ballots is accurately counted by electronic counting machines.

- Conducting a Process and Results Verification for Transparency (PRVT) to validate the accuracy of the official result based on a random sample of polling station results.[5]

While in some cases the EMB can conduct audits, either directly or by contracting external experts, some are more appropriate to be conducted by independent, nonpartisan citizen election observers.

Model Questions

- Were audits conducted on all, some or none of the election technologies used during the electoral process?
- Does the legal framework require audits to be conducted if certain criteria are met? If these criteria were met, were audits conducted?
- Did the audit have a broad scope, or was it limited in nature? Were there significant aspects of the technology that was not subject to an audit?
- Did the EMB engage independent experts in the audit process? Was the process to select the experts transparent and inclusive? Did the experts have access to the full technology solution, or were any components off-limits?
- Were the audits' methodology and findings shared publicly? Did political contestants, civil society and other actors have an opportunity to provide feedback on the methodology prior to the audit being conducted?
- Were the audit methodologies appropriate to determine the performance, functionality, or cost-effectiveness of the system?

Post-Election Review and Inter-Election Processes

The end of the election cycle also provides an opportunity to assess whether technology used in the process contributed to its integrity and credibility, or if there were shortcomings that should be addressed prior to the next election. While post-election assessments should be led by the EMB, they should include the active participation of critical stakeholders.

[5] Process and Results Verification for Transparency (PRVT) is an election day observation methodology that allows nonpartisan citizen organizations to systematically assess the quality of opening, voting, closing, and counting – as well as official results and, indirectly, the tabulation process – at a national scale and independently verify official results. Using statistical principles and rapid reporting technologies, PRVTs enable citizen observers to provide accurate, timely, and comprehensive information about the conduct of election day and, when appropriate, to quickly estimate where credible results of the election should fall. More information is available at www.ndi.org/prvt.

Model Questions

- Did the EMB conduct an assessment to determine if the technology solution successfully addressed the problem identified at the beginning of the process?
    - Was this process inclusive of candidates, political parties, ordinary citizens, citizen and international observers, and journalists?
    - Did the technology work as expected regardless of environmental factors, such as polling stations located in different climates or with different access to the internet?
    - Did the technology work consistently given the same input? For example, did a biometric voter identification device respond consistently when reading the same fingerprint, or did a vote counting machine consistently allocated a vote to the same candidate when the same bubble was filled in multiple ballots?
    - Did the assessment identify any risks to electoral integrity, barriers to the participation of eligible voters and other actors, or reduced the transparency or accountability of the process that would need to be addressed in future elections?
- Did the EMB define a process to ensure the system is ready for future elections, including by leveraging its strengths and mitigating shortcomings?
- If the technology was adopted as part of a pilot, are there any specific steps that need to be taken to scale the technology to a higher-level election with a broader geographic scope?
- How is the EMB planning to maintain the hardware and software to ensure they are operational and updated for future elections, including digital and physical security?

Section II: Specific Electronic Election Technologies

While the criteria and questions mentioned above are applicable to all technologies, specific technological solutions could introduce distinct risks that require targeted lines of inquiry. When designing your strategy to monitor these technologies, be sure to take into consideration both the cross-cutting issues in Section I, and specific questions outlined below.

Voter registration

In nearly all countries, the voter registry is maintained in an electronic format. The manner in which voter information is entered into that registry, and what information it contains, differs by country. For example, some countries gather voters' biometric information, such as fingerprints or facial features, which are then used to detect duplicate registrations or validate citizens' identity on election day. Electronic voter registries can reduce the risk of transcription errors, make it easier to assign voters to polling stations and allow EMBs and other actors to conduct analysis to identify issues such as duplicate voters.

In some countries, voters can complete all or part of the voter registration process online, while in other countries they must physically visit a particular location to register, which might include an electronic component and/or paper forms.

Model Questions

- If voter registration staff complete data entry based on information given by voters verbally or in writing, what measures are in place to minimize clerical errors and standardize data entry?
- How is voter information transmitted to a central location? What security measures are in place to ensure that the voter information is not compromised?
- How is voter information stored? Is it stored on the registration device directly? Is it also transmitted onto a cloud-based server? How is the data protected at the machine level, during transmission and the central level?
- If biometric information is being collected, what measures are in place to protect the data security of this sensitive information?
- If biometric data is used to analyze or clean the voters list, what is the list maintenance process? What measures are in place to ensure that voters are not erroneously disenfranchised due to failures in technology?
- Do voters have the ability to check their registration online or using other technology?
- Is the voters list shared with political actors and other stakeholders? How is transparency balanced with maintaining voters' privacy?

Candidate Nomination and Ballot Qualification

Candidate nomination and ballot qualification processes can use technology in a variety of ways to render the process more efficient or accessible. Some countries use systems of sponsorship, requiring a certain number of signatures from voters for candidates to be nominated or qualify for the ballot. In these cases, technology may be used to analyze voter signatures to determine their accuracy or authenticity. Other countries have online systems for parties or candidates to submit lists for proportional representation systems. In some countries, candidates submit their application for nomination electronically, while in others, a paper application must be physically presented to the EMB or other body managing candidate nominations.

Model Questions

- For sponsorship systems where software is used to analyze signatures, is there a manual backup to check inconsistencies? Can this system be audited?
- For instances where candidate lists are submitted electronically, does the software prevent parties or candidates from submitting lists that do not comply with requirements such as gender quotas?
- Does the technology include a mechanism for making sure that applications are complete and meet all requirements?
- Does the EMB provide training for candidates or parties on how to use the system?
- Did the system improve efficiency and/or accessibility of the candidate nomination or ballot qualification process? Was there a change in the number of candidates or parties nominated or qualified for the ballot from previous elections?
- Is information on candidate registration available online, including candidates who were rejected and why?

Voter Identification on Election Day

In an effort to overcome perceived challenges of voter impersonation or fraud, some EMBs have introduced technology to **verify voter details on election day**. This system relies on the use of biometric data, often face scans and/or fingerprints, collected during the voter registration process to verify the identity of voters on election day. Through the use of Biometric Voter Identification (BVI), EMBs can more easily record voting turnout and demographics and at the same time limit multiple voting and other perceived challenges. However, if the technology and systems used to identify voters is not adequately calibrated and/or malfunctions on election day, eligible voters could be disenfranchised, and the credibility of the overall election process may be undermined.

Model Questions

- Is there robust and transparent testing of all voter authentication or verification devices? This includes connectivity and offline functionality, appropriate voter information storage, and the accuracy and consistency of digital recognition.
- What redundancies and back-ups exist in case of device or system failure? Were those policies followed on election day?

- Have critical stakeholders, including voters, been adequately sensitized and educated on how the system functions and what happens in instances of limited or widespread failure?
- Did the system appropriately and consistently function on election day? Were there issues of registered voters not being identified through the BVI?
- Are there measures in place to prevent unauthorized access to voter information via the authentication or verification devices?
- If voters are identified using biometric information (such as their finger/thumb print or facial recognition technology, how is biometric data used?
  - Is the biometric system potentially being used to disqualify voters? If so, what recourse is available in case an eligible voter is disenfranchised?
  - If voter ID cards have photos on them, how does the EMB train its staff to identify voters based on their photos?
  - If the EMB uses technology to identify potential underage voters based on their photos, how do they ensure the accuracy of this assessment?
- Were any voters prevented from voting because the voter identification device indicated that they either were not registered to vote in that precinct, or that they had already voted?
- Did the use of biometric identification make the voting process more efficient? Did it create new bottlenecks that resulted in a slower process?

Broadcasting the Voting Process

In certain contexts, concerns over election day manipulation have resulted in the introduction of **polling station webcams**. Governments and EMBs have claimed that live streaming the voting and counting process of polling stations reduces the likelihood of electoral fraud and manipulation. However, electoral fraud and malpractice can occur at any point during the electoral cycle. The use of webcams could cause the public to focus too much on only a limited portion of activities (i.e., only those visible on the webcam on election day) in assessing whether the conduct of elections deserves their trust and confidence. The introduction of webcams have also raised concerns that cameras will be used as a way to intimidate and identify voters, citizen observers, and political agents, ultimately resulting in a chilling effect for election day participation.

Model Questions

- Were key stakeholders provided the opportunity to monitor installation and testing?
- Were cameras present and functional in all polling stations?

- Was the system operational during the entirety of the voting and counting process?
- Was the secrecy of the ballot maintained at all times via live stream feeds?
- Were system challenges resolved in a timely and effective manner on election day?
- Was video footage ever used for an electoral challenge or to report a violation?
- Was video footage ever used in bad faith to intimidate voters, party agents, or other stakeholders?

Electronic Voting

Electronic voting, often referred to as e-voting, is viewed as a mechanism to increase efficiency, inclusivity, and trust in the election process. E-voting relies on the use of technology for voters to make and record their ballot choice, which is then stored on the machine, recorded as a token, and/or transmitted to an offsite cloud server. In some cases, voters use ballot marking devices to electronically select their preferred candidate and produce real ballots that allow voters to ensure their choice was accurately reflected. These ballots are then processed and counted electronically. While e-voting attempts to increase voting and tabulation speeds, reduce errors, and make voting more accessible to persons with disabilities and other barriers, it is highly complex and demands a high level of infrastructure, digital security, and citizen trust in the process. Ineffective implementation of e-voting undermines the integrity of the overall electoral process and may impact key stakeholders’ willingness to utilize costly technologies in the future.

Model Questions

- How are voter ballots cast and recorded? Does this maintain secrecy of the ballot? Does the machine allow for audits or recounts?
- Does the machine offer a voter-verified paper audit trail (VVPAT), or other non-digital confirmation of a voter's choice?
- How does the system ensure that cast votes are not lost or compromised in case of system failure?
- What redundancies and back-ups exist in case of device or system failure?
- Have critical stakeholders, including voters, been adequately sensitized and educated on how the system functions and what happens in instances of limited or widespread failure?
- Were critical stakeholders provided opportunities to monitor, inspect and demo the electronic voting machines well ahead of election day?
- Did the system function appropriately and consistently on election day?
- In cases where there is technology malfunction or failure were policies adhered to?
- Did the system improve accessibility for voters?

- Were rates of invalid ballots lower for polling stations that used electronic voting machines as opposed to other methods, or as compared to previous elections?
- Did the technology help reduce the time citizens needed to cast their votes? Did it introduce new bottlenecks that resulted in slower voting times?

Ballot Counting

Ballot counting machines continue to be utilized across the globe to aggregate and finalize vote totals. These machines minimize the human element of counting ballots, since each marked ballot is fed through an optical reader to tally results. However, depending on how voters mark their ballots, the machine may misread some ballots as invalid, which would require a human decision to be made about validity. In contexts where ballot counting systems are separate from the method to mark votes, voters use either paper ballots or an electronic ballot marking device, allowing for a clear paper trail, re-counts, and audits, but alleviating concerns surrounding manipulation or corruption during the counting process.

Model Questions

- Were key stakeholders, including citizens and political parties provided with an opportunity to see and understand how the machines work ahead of election day?
- Did the EMB plan for and implement appropriate digital security protocols to protect the counting process?
- Was the system operational during the entirety of the counting process?
- Was the secrecy of the ballot maintained at all times during the counting process?
- Are there provisions in place to review ballots marked as invalid by the counting machine?
- Are there provisions in place – either as default, based on thresholds, or upon request – to conduct manual counts in some or all polling stations, either in parallel with the electronic count or as a separate recount? Were there any inconsistencies between manual and electronic counts? How are any inconsistencies resolved?
- In polling stations with more than one counting machine how is the protocol for the entire polling station generated?

Results Transmission and Publication of Preliminary Results

EMBs are increasingly relying on technology to **transmit preliminary election results** on election night and the following days. If implemented successfully, these efforts allow EMBs to **publish preliminary results online** soon after the close of voting to avoid an information vacuum and mitigate the risk of increased tensions or violence. However, malfunctions of either the results transmission or the publication platform, unexpected delays or other challenges could instead increase mistrust in the system and the overall process. By contrast, publishing timely, granular information from individual polling stations – including voting results and copies of official results protocols – allows political contestants, citizen observers and other actors to compare preliminary results with information collected at the polling station level, helping increase trust in the process as warranted.

Model Questions

- Is the legal framework clear about which results will be considered official, in cases where there is both electronic transmission and offline transmission?
- Was there a robust and transparent plan to test all aspects of the results transmission system, including the transmission channels, software and hardware stability, server load management and connectivity at the polling station?
- What measures are in place to strengthen the cyber security of the system?
- Were political parties, candidates, citizen and international observers, the media, and academics able to monitor the implementation and testing of the system?
- Did the EMB establish a clear timeline and process for the reception and publication of preliminary results?
- Was the system operational shortly after the official end of the voting process?
- Does the online results publication platform include preliminary results disaggregated by polling station, and aggregated for different administrative levels (e.g. municipalities, provinces, countrywide)?
- Does the platform include a scanned copy of the polling station-level results protocol? If so, are protocols typically legible?
- If ballots are counted electronically, are results transmitted by each individual counting machine or for the entire polling station?
- Are preliminary results, disaggregated by polling station, available in machine-readable format(s), such as comma separated values (CSV) files, Excel files, or through an application programming interface (API)?
- In the event of delays or system failure, did the EMB proactively communicate about the causes, and plans to address the problem?

Official Results Aggregation

Often, **aggregation of official results** occurs at one or more administrative levels before they are certified. To reduce opportunities for arithmetic errors, EMBs can deploy electronic systems that officials can use to enter and aggregate results from lower-level administrative units. This is especially useful in countries that allow voters to select many candidates for parliamentary or council elections, which could provide opportunities for human error in the collation of results. Similarly, in countries using proportional representation systems, the allocation of parliamentary seats based on votes received by parties and candidates is a sensitive process. Using algorithms that can be reviewed by contestants and observers can increase trust in the process and the outcome of the election.

Model Questions

- Were political parties, candidates, citizen and international observers, the media, and academics able to monitor the implementation and testing of the system?
- Did the EMB establish a clear timeline and process for the aggregation and publication of official results?
- Did the system work as expected at all administrative levels?
- Were representatives of candidates, political parties, the media and accredited observation groups able to observe the aggregation process and verify the aggregated results?
- Are official aggregated results, disaggregated by lower-level administrative units, available in machine-readable format(s), such as comma separated values (CSV) files, Excel files, or through an application programming interface (API)?
- In case of proportional representation elections, is the results aggregation system used to allocate seats among contestants? Has the seat allocation system been thoroughly and transparently tested to ensure that calculations are accurate and in accordance with the law?

Conclusion

As use of technology in elections continues to spread around the world, citizen election observers increasingly need to become well versed in the impact technology can have on electoral processes in their country. Observers, and the broader community of electoral stakeholders, must consider both the relative benefits and the challenges to the inclusiveness, transparency, and accountability of an electoral process that are introduced when technology comes into play.

However, while observers need to become familiar with the technology under consideration, this does not mean that every observer or observer organization needs to have highly technical expertise in electronic technologies, such as understanding source code. While the functionality of the technology is important to consider, the process through which the technology is adopted is equally critical to the credibility of the electoral process — including the decision to adopt technology, updates to the legal framework, procurement, design and development, testing, staffing, training, certification, audits, dispute resolution, and post-election reviews. To comprehensively monitor the adoption of electronic technologies and assess their impact on the electoral process, observers will need to engage in the process early and look at it from a global perspective, focusing not only on what technology is adopted, but the reasons why — and whether the new technologies enhance the integrity of the electoral process.