

E-Voting in UAE FNC Elections: A Case Study

Dr. Ali M. Al-Khouri
Emirates Identity Authority, Abu Dhabi, United Arab Emirates
E-mail: ali.alkhouri@emiratesid.ae

Abstract
Electronic voting (e-voting) has been attracting the attention of governments around the world. Many countries have pursued implementing e-voting systems in their national elections. This article presents a case study of an e-voting system deployment in the United Arab Emirates (UAE). The UAE has conducted its Federal National Council (FNC) elections for the 2011-2015 session of the National Assembly using an advanced e-voting system with biometric-based smart cards to verify voters' identities. The article provides detailed insights on the phases of the project, from the design phase up to election day. The article also provides a comprehensive overview of the current literature around e-voting in order to enhance understanding of the field and of global practices.
Keywords: electronic voting, UAE FNC elections, national identity.

1. Introduction

Electronic voting is gaining in popularity around the world. It has become well-established in countries such as Belgium and Switzerland, and has been deployed in many European countries like UK, Denmark, France, Ireland, etc. Electronic voting has been considered to be an efficient and cost-effective alternative compared to the traditional classic voting procedures (IPI, 2001). See also Figure 1. Electronic voting technologies that have been in use varies from punch cards, optical scan voting systems and specialised voting kiosks, including self-contained direct-recording electronic (DRE) voting systems. Additional technological components may also enable the transmission of ballots and votes via telephones, personal handheld computer devices, and the Internet.

The purpose of this article is to provide a more thorough analysis of a government e-voting system deployment experience. The case study provides an overview of the UAE Federal National Council (FNC) elections that was based on an advanced e-voting system. The voter-recognition system in the UAE FNC elections was based on a smart card with biometrics and public key cryptography.

The structure of this paper is as follows; in section 2, we describe the methodology adopted. Section 3 presents an introduction to the concept of elections and voting, and the different approaches to voting. Section 4 provides an overview of the existing literature around e-voting. Section 5 provides a brief glance at e-voting systems deployment experiences around the world. Section 6 presents the UAE FNC elections case study, outlining the different phases of the project, from the design phase up to election day. Section 7 presents some key factors that contributed to the overall success of the elections. In section 8 we outline some lessons learnt from the implementation of the UAE FNC e-voting system. Finally, in section 8 we draw some conclusions and provide some pointers for future work.

2. Research Methodology

The research content presented in this article aims to provide an understanding of the issues surrounding the use of electronic voting in practice. It thus provides a review of the existing literature in the field of e-voting to outline some of the critical points in the current body of knowledge. The researcher uses an action-based case study method to provide a contextual analysis of a recent government implementation of an e-voting system. Indeed, there is a continuum between the "describer" of case studies and the "implementer" of action research (Waddington, 1994).

The case study method was used to describe relationships that exist in reality (Yin, 1984) and to produce an understanding of the context of the information and the process whereby the information system influences and is influenced by the context (Walsham, 1993). Action research aimed to develop outcomes and solutions that are of practical value to the stakeholders with whom the research is working, while at the same time developing and contributing to the existing body of knowledge (Rapoport, 1970; Susman and Evered, 1978).

The senior role of the researcher in the reported project as a member of the higher national election committee, and head of the technology team, as well as a member of other management and legal committees, enabled him to have a more in-depth and working view of the case, and acquire understandings of specific situations. In addition, the researcher's fieldwork involved the design of the system and the overall observation of the implementation case, from the early phases of preparation, design, during the run-up to the election and on the actual polling day.

An agile project and system development methodology was adopted, which is discussed in some detail in section 6.3. Semi-structured workshops with key stakeholders and commercial suppliers' staff were undertaken before the system implementation to allow for government concerns and requirements to be addressed. The researcher's observatory role on election day took place at the operations management centre, which was set up to handle the technical and organisational issues that arose. The researcher was also part of the verification processing team at the end of election day. All this supported the research work and provided the opportunity to acquire hands-on experience of the implementation, management, and administration of the e-voting system.

3. Elections and Voting

An election is a formal decision-making process by which a population chooses an individual(s) to hold public office position(s) (Britanica, 2012). Elections are associated with the term "Electoral reform", which describes the process of introducing fair electoral systems, or improving the fairness or effectiveness of existing systems that should altogether reflect the public opinion.

Electronic voting is a term that may encompass several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. Electronic voting systems were first debuted when punched card systems were introduced for the 1964 presidential elections [Saltman, 1975]. Then, optical scan voting systems emerged that allowed computer systems to count voters' marks on ballots, i.e. direct-recording electronic (DRE) voting machine.

DRE voting machines collect and tabulate votes in a single machine, and have been used in elections in Brazil and India, and also on a large scale in Venezuela and the United States. They have also been used on a large scale in the Netherlands, but have been decommissioned after public concerns. There has been controversy, especially in the United States, that electronic voting, especially DRE voting, can facilitate electoral fraud.

Nonetheless, the concept of e-voting has been gaining popularity in many countries. Windley (2005) accounts the lure of e-voting and the growing applications of digital technologies to voting systems, to the simple idea that computers, and the Internet, have fundamentally changed other parts of our lives; he states that, since voting is one of the basic processes of democracy, it seems a natural candidate for electronic automation.

Advocates of e-voting argue that the use of advanced information technologies not only speeds up the counting of ballots, but also brings about advanced features of uniqueness, accuracy, completeness, verifiability, auditibility, privacy, and uncoercibility.

In general, two main types of e-voting can be identified:

- **e-voting**: physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations); this is the most common and preferred approach (see also Table 1 for e-voting systems); and
- **i-voting**: also referred to as remote e-voting, where voting is performed within the voter's sole influence, and is not physically supervised by representatives of governmental authorities (e.g. voting from one's personal computer, mobile phone, television via the internet). Internet voting systems have gained popularity and have been used for government elections and referendums in the United Kingdom, Estonia and Switzerland, as well as municipal elections in Canada and party primary elections in the United States and France.

There are also hybrid systems that include an electronic ballot marking device (usually a touch screen system similar to a DRE) or other assistive technology to print a voter-verified paper audit trail, then use a separate machine for electronic tabulation..

Table 2 provides an overview of the typical strengths and weaknesses that different e-voting solutions tend to have compared to paper-based equivalents (Internet voting vs postal voting; voting machine vs paper voting in controlled environments) (IDEA, 2011).

4. Literature Review

The amount of reported work on the subject of e-voting is considerably significant. The literature of electronic voting states that the field needs significant improvement (Alexander, 2001; Besselaar and Oostveen, 2003; Cranor, 2000; IPI, 2001; Hargrove, 2004; Liptrott, 2006; Manjoo, 2003a; Manjoo, 2003b; Millar, 2002; O'Donnell, 2002; Oostveen and Besselaar, 2006; Shamos, 1993; Xenakis and Macintosh, 2006). Advocates of e-voting point out that electronic voting can reduce election costs and increase civic participation by making the voting process more convenient. Critics maintain that without a paper trail, recounts are more difficult and may open the door for electronic ballot manipulation, and that even poorly-written programming code, could affect election results. Many researchers have produced different studies and approaches to address these concerns. A sample outline of such research is provided in Table 3.

A report worthy of note around e-voting was produced by an MIT Universality Team in the United States.

The Caltech/MIT Voting Technology Project that was established in December in 2000, following the controversial election recount of the 2000 presidential vote in Florida, assessed the magnitude of the problems surrounding voting systems, their root causes and how technology can reduce them (Caltech-MIT, 2001). The report provided a set of recommendations on the various issues related to voting and proposed a framework for a new voting system with a decentralised, modular architecture in which vote generation is performed separately from vote casting. The report emphasised the importance of developing a permanent audit trail. It also stressed the fact that the vote generation machine can be proprietary, whereas the vote casting machine must be open-source and thoroughly verified and certified for correctness and security.

The National Institute of Standards and Technology draft report, issued in 2006, proposed vote verification through a parallel process of electronic and ballot count (NIST, 2006). It indicated that voting systems should allow election officials to recount ballots independently from a voting machine's software. The recommendations endorse "optical-scan" systems in which voters mark paper ballots that are read by a computer, and electronic systems that print a paper summary of each ballot, which voters review and elections officials save for recounts. NIST indicated in its report that the lack of a paper trail for each vote "is one of the main reasons behind continued questions about voting system security and that it diminished public confidence in elections."

The California Internet Voting Report [CIVTF, 2000] suggested an innovative strategy to enable remote internet voting to improve participation in the elections process, i.e. providing voters with the ability to cast their ballots at any time from any place via the Internet. On the contrary, experts argue that the internet isn't ready yet for "prime time" national federal elections over the internet, given the current state of insecurity of hosts and the vulnerability of the Internet to manipulation and denial-of-service attacks (Hisamitsu and Takeda, 2007; Kosmopoulos, 2004; Rubin, 2002; Schneier, 2004). They also identify security issues in social engineering and in using specialised devices and other factors that could undermine the sanctity of an Internet-based election process, and that the current infrastructure is inadequate for remote Internet voting (ibid).

Another report produced by the National Institute of Standards and Technology (NIST) in 2008 concluded that widely-deployed security technologies and procedures could mitigate many of the risks associated with electronic ballot delivery, but that the risks associated with casting ballots over the Internet were more serious and challenging to overcome (NIST, 2008).Another recent NIST report (2011) concluded that Internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems.

Other researchers point out that building secure online voting systems is far from being possible and that a small configuration or implementation error would undermine the entire voting process (Wolchok et al., 2012). Reference is made to the pilot project of an online voting in Washington, D.C. and how researchers at University of Michigan were able to break through the security functions and gained complete control of the election server in less than 48 hours. Researchers argue that fundamental advances still need to be made in security before e-voting will truly be safe (Cramer et al., 1996; Ikonomopoulos et al., 2002; Schoenmakers, 1999; Wolchok et al., 2012).

Researchers indicated that operationally, no commercial system is likely to ever meet all requirements, and that developing a suitable custom system would be extremely difficult and prohibitively expensive (Neumann, 1993). Others indicated that any catastrophic failures and sweeping fraud made possible by imperfections in electronic voting machines are also likely to occur in a real election(Shamos, 1993).

Shamos (1993) refers to the fact that the real source of election problems is the result of human limitations. He describes that the chief source of the issue is the willingness of unsuccessful politicians to embrace any conceivable reason for their loss, except that the voters didn't want them. His reflective recommendation proposes that government efforts expended in meeting threats to the election process should be rationally related both to the probability of the threat and the seriousness of its effects.

Other researchers argue that the progress of e-voting relies on the advancement of standards and technical solutions, which should take into account discussions on general requirements, threat perceptions and the economic, political and sociological implications surrounding the use of electronic voting systems (Alexander, 2001; Cranor, 2000; Hillman, 2007; Hoffman, 2004; Jones, 2001; Shamos, 1993; UK POST, 2001; Volkamer, 2009). Rubin (2002) argues that technologists should take on a role to educate the policymakers about the issues surrounding an e-voting system and enable them to develop more effective strategies.

Another part of the literature deals with public trust and confidence. It argues that, if the public perceives elections to be unfair, the foundation of the government is weakened. Whether electronic voting systems are fair may not even matter; it is the public perception that is crucial (Bonsor and Strickland, 2011).

On a different standpoint, the International Institute for Democracy and Electoral Assistance published a policy report that identified some essential considerations for e-voting systems to gain public trust and confidence (IDEA, 2011). It introduced a pyramid of trust that consists of three levels: credible electoral process, socio-political context, and operational and technical context. See also Figure 2.

The top level represents the ultimate goal of the electoral reform and the introduction of the e-voting system, and is a factor that is dependent on the two levels shown below. Public trust is seen to be determined by the socio-political context in which e-voting is introduced. Some factors in this context can be directly addressed by a comprehensive e-voting implementation strategy, while others, such as a general lack of trust in the Election Management Body (EMB), or fundamental political or technical opposition, will be more difficult to change. A negative socio-political context has the potential to create serious risks, even if the technical and operational foundations of the e-voting solution are sound.

Chiang (2009) developed a technology acceptance model that constitutes four trust variables, namely ease of use, perceived usefulness, attitude of usage, and security. The research results showed the effect of 'ease of use' on voters' attitude towards using the e-voting system required 'perceived usefulness' as a medium. Then, the effect exhibited positive and significant influences among ease of use, perceived usefulness and attitude towards using the e-voting system. Security of the e-voting system has a positive and significant effect on attitude and trust in the e-voting system. The study concluded that the security of the e-voting system plays an important role in establishing user trust. Overall, the literature identified key elements that e-voting systems need to heed. These are listed in Table 4.

Though debate on the issue of e-voting has been and will continue to be passionate, most critics recognise that a move towards an electronic voting system is an inevitable step in the evolution of the voting process (2007).Governments seem to be motivated to adopt e-voting systems, despite the issues and concerns reported in the literature, as the next section will present.

5. e-Voting Deployment around the World

> "No one would buy a safe that could easily be opened, but everyone who has ever bought a safe has bought one that can be cracked. The same is true for voting systems. The issue is not whether they are secure, but whether they present barriers sufficiently formidable to give us confidence in the integrity of our elections." (Shamos, 1993)

Despite what the literature raises in terms of risks and the reasons why not to go for electronic voting systems, governments worldwide seem to be motivated to implement these systems. The following world map depicts the adoption of the e-voting systems across the world, as well as some examples of e-voting trials and uses worldwide.

As we can see from the map in Figure 3, though countries in the west had initiated e-voting, developing countries have taken some noticeable lead in adopting e-voting systems at a national level for their election systems. In fact, e-voting system adoption seems to be closely associated with the maturity in the election processes worldwide. The following sub-sections will highlight the use of electronic voting systems in Australia, India and Estonia.

5.1 Australia

Australia has the distinction of compulsory voting adopted at the Federal and State levels. Every enrolled eligible voter must vote. Failure to vote can lead to legal implications and fines. Driven by this need of compulsory voting, Australia first used the remote voting by electronic means in 2001. In the subsequent elections of 2004, 2007 and 2010, widespread usage of technology ensured successful deployment of electronic voting. The desire to include all sections of eligible voters, backed by the compulsion in voting, made Australia adopt i-voting as (assisted voting) for the visually impaired voters. The i-voting system is also available for Australians who live overseas. As a result, Australia is now firmly entrenched in the world map of e-voting as a pioneer in adopting e-voting systems.

5.2 India

India is another example of a large nation with eligible voters. India is unique in its size and complexity and the sheer logistics support required to conduct nation-wide elections. It follows precinct voting, as in many countries. There are nearly 740 million eligible voters spread across nearly 830,000 polling booths. Certain sections of the Indian elections were plagued by voting malpractices and fraudulent voting. Handling, managing and manning 1 million polling stations, as well as the paper ballots and ballot boxes, posed severe security problems.

India first adopted electronic voting machines (EVMs)in 1982, allowing voters to cast their votes in electronic machines in about 50 polling stations. Indeed, the country has come a long way in deploying the EVMs. Since 2004, Indian elections have been using EVMs fully and it is reported that, in the 2009 general elections, 1,368,430 EVMs were used. It is now mandated for the EVMs to be provided with ballot printouts for paper audit trails. In 2011, Gujarat State was the first Indian state to adopt and use Internet voting for the state elections, with around 26 million eligible voters.

The success of Indian electronic voting systems can be gauged from the fact that, today, countries like Bhutan, Nepal, Kenya, and Fiji are set to use these EVMs with India exporting the machines, technology and the resources. While Australia continues to use EVMs in precinct voting mode, India is moving to a hybrid mode of

EVMs and i-voting. Large-scale urbanisation, Internet availability and accessibility and encryption technologies are making it possible for India to begin utilising i-voting.

5.3 Estonia

Estonia is a classic example of a country leveraging technology in conducting national elections using i-voting. Central to their theme was the issuance of an ID card with PKI (digital certificate) capabilities for voter identification, authentication and, finally, casting an encrypted vote ensuring privacy and voter secrecy combined with anonymity.

The digital certificate in the ID card in Estonia is envisaged to enable the voting system to more robustly verify the credentials of the cardholder. The certificate itself is submitted to the voting system through the card using the cardholder's PIN. The certificate is verified for authenticity and validity. Once validated and authenticated, the user is provided access to the on-line voting site. The voter selects the candidate and submits the vote. The vote submission is akin to the voter sealing the paper ballot in a secure envelope and dropping it into the ballot box. The digital certificate is used for digitally signing the vote and encrypting, using the private key of the card holder and the public key of the e-voting system. The vote, thus, is submitted as if sealed in a secure envelope. At the server end, decryption of the vote takes place using the election keys, while the signature validity of the voter is checked. At no point is the voter's identity revealed.

Overall, the key success factors for e-voting and i-voting systems in these countries are considered to be due to the (1) existence of a legal framework and legal validity of the use of these systems, and (2) the availability of an audit trail of the counted votes. The later point enables the voter to go back to the voting system to check and confirm if his/her vote was indeed considered in the counting of the votes.

From our reading of the existing practices, it is interesting to note the factors that have driven countries to adopt e-voting systems. Each country is driven by different factors that were key in their adoption of the e-voting systems. Australia is driven by its need to ensure "inclusive voting" – that is, every eligible voter should be able to vote and should be provided with the access and ability to vote. This includes overseas Australians, visually impaired citizens, etc. This is as a result ofits rule of "compulsory voting".

India is driven by its need to contain election fraud and to reduce the complexity in the logistics of handling manual ballots. Estonia is driven by its need for providing citizen convenience and to increase voter participation. The elections conducted in Estonia were beset with problems of low voter turn-out.

The USA has moved to machine-based (EVM) e-voting primarily because of the problems it faced with the punch card voting systems in 2000. The Florida elections were found to have discarded votes, which otherwise were eligible votes and, had they been counted, the elections results would have seen a different conclusion.

France, Germany, and Belgium have basically taken advantage of their home-grown technologies and adopted e-voting systems. Brazil had similar issues as in India, but the adoption of DRE (Direct Recording Electronic Voting) Machines were used which were far different from the EVMs used in India. Thus, our understanding is that local political needs and socio-economic factors contributed to the adoption of e-voting systems in different countries.

The purpose of this section was to provide a short overview of some successful implementations of electronic voting systems globally. The next section will present the main content of this article, namely the use of an e-voting system in the UAE FNC elections.

6. UAE FNC Elections

On 2 December 1971, with the adoption of the constitution, the federation of the United Arab Emirates was officially established. A few months later, in February 1972, the country's first ever federal national council (FNC) was set up as the country's legislative and constitutional body. The FNC consisted of forty members appointed by the rulers of each of the seven emirates.

In 2005, the UAE had its first national elections. The presidential resolution stipulated that half of the FNC members (out of 40 members) would be elected by citizens and the other half would be appointed by the Ruler of each Emirate. This was recognised as a step forward to enhance a well-structured political participation in line with citizens' aspirations, and as a major milestone towards modernisation and development of the federation.

Indeed, the introduction of this partial election system was seen as the first step in a gradual process aimed at empowering and enhancing the role of the FNC, and developing more effective and vital channels for coordinating between the FNC and the government, thereby opening new prospects in the parliamentary life of the UAE. In the first electoral experience in the UAE in 2005, the NEC approved electronic voting instead of traditional voting procedures.

The same election model was used for the 2011 FNC elections, except for the electoral college, where the number of voters increased from around 6,000 to almost 130,000. The 2011 FNC elections were considered to be more challenging due to the short time frame and the size of the electoral college, as well as the fact that the majority of voters were first-time voters and had never seen a ballot box (see also Figure 4). The government

decided to take innovative steps to encourage participation and introduced technology-driven systems to facilitate the overall program.

6.1 Forming a National Election Commission (NEC)

Organisation is an important element of the overall management process. It is next to planning in importance. Organising involves the integration of resources in order to accomplish the objectives. In management terms, organisation is both the process as well as the end-product of that process, which is referred to as organisation structure. The success of the management process will be determined by the soundness of the organisation structure. Therefore, such structure acts as the foundation on which the whole super-structure of management is built.

Clearly, a sound organisation structure was fundamental to ensure that the elections management activities are conducted in an efficient and effective manner. A National Election Commission (NEC) was formed in February 2011 (7 months before the elections) by a presidential decree consisting of 10 government officials representing key government organisations and entities that were envisaged to support the efforts of regulating the electoral process in additional to three public figures. The NEC was empowered to oversee the whole election process, including:

- Setting out the overall Election Framework
- Supervising the elections
- Supporting efforts to raise electoral awareness
- Developing elections guidelines
- Locating Polling Centres in each Emirate
- Approving regulatory measures for establishing the electoral legal framework
- Issuing and seeking approval for the governing rules for the lists of Electoral Panels Members
- Setting the date of elections.

Current research states that defining roles and responsibilities within the e-voting system implementations could provide a better understanding of who is responsible for doing what in the different process stages so that the planned election result is produced (Xenakis and Macintosh, 2006). As such, the commission developed an organisation structure with 20 sub-units to support the elections program. With the flat hierarchical organisation structure, the National Election Commission (higher committee) was responsible for establishing strategy and overall direction, whilst the lower level units had the responsibility for a specific function, as illustrated in Figure 5. More details about the functions and responsibilities of each unit in the structure are provided in Annex-1.

6.2 Opting for an e-Voting System

The National Election Commission opted for introducing an advanced electronic voting system for the conduct of the 2011 elections. The national identity management infrastructure maintained by the Emirates Identity Authority (EIDA) was seen to construct the primary foundation for the desired e-voting system and enhance its overall security, i.e. (1) the use of the Population Register: to extract the electoral roll of eligible voters, and (2) the utilisation of biometric-based smart identity card issued to citizens (e-ID Card) to authenticate the voters.

It was also decided that the e-voting system would be developed with a de-centralised architecture. This was because of concerns over the permanence and stability of the e-voting system, lack of reliability on the internet communications, and to ensure continuity and simultaneous operations of the electoral process. This was in line with recommendations reported earlier in the existing literature.

Most of the Emirates had multiple voting centres for contingency and capacity-planning purposes. Voters were expected to visit the polling centres in their representative Emirate of domicile to cast their votes. The information of each voting centre was synchronized with the voting centres within that emirate. The aggregated participation information per Emirate was sent manually to the Main Abu Dhabi site, but the ballots of each Emirate were not synchronized to the main Abu Dhabi site. See also Figure 6. The following section will outline the e-voting deployment methodology.

6.3 E-Voting System Deployment Methodology

The UAE FNC elections were planned to occur on only one day. The challenge was in getting the system right from the beginning. Besides, the new electronic voting process was envisaged to promote integrity, accuracy, time savings, reliability, accessibility, and auditability. Thus, there was a clear need for systematically developed requirements specifications for the e-voting system, which took into account the requirements imposed by the existing legal framework, the functionality reflected by the conventional voting procedures, and the required security attributes that the system should exhibit.

The project team applied an agile methodology to elicit requirements specification in an accepted format. The agile development methodology was adopted for the design, development, deployment and implementation

of the e-voting system. Semi-structured workshops with key stakeholders and commercial suppliers' staff were undertaken before the system implementation to allow for government concerns and requirements to be addressed.

The adopted agile development stressed rapid iterations to the e-voting system, as well as evolving requirements facilitated by direct user involvement in the development process. It provided a framework by which to visualise scope, orchestrate mundane and repetitive development tasks, and enforce process. See also Figure 7.

6.3 e-Voting Business Process

Multiple workshops were conducted to articulate and document business processes. Requirements were elicited through a set of use cases, along with specifications of similar systems implemented worldwide. These were later translated into functional requirements for the e-voting system design. See also Table 5 for adopted design principles.

The primary input for the business processes was taken from the UAE Elections Legal Framework that was reviewed and approved by the Federal National Election Commission. It basically outlined the overall electoral processes. In general terms, the following were identified as the main requirements for the e-voting system:

- Authentication of the voter will rely on the UAE e-ID card;
- De-centralised vote feature will be implemented in each Emirate, which will be synchronised with the central database;
- A voting sequence should allow a selection of candidates up to the number of candidates valid for each Emirate;
- Ballot copy with vote cast will be printed for audit purposes;
- Ballot copy will contain: election banner, Emirate, voting centre, candidate(s) selection (Number and Name).

  See also Figure 8.

On the other hand, the business processes related to the e-voting system were categorised in three different stages, as outlined in Figure 9and explained below.

6.3.1 Pre-Election Period:

a) **Electoral College**: The electoral college represented the selected electors (also referred to as 'electoral roll of eligible voters') who would vote for the candidates in their representative Emirates. Each of the seven Emirates had its own electoral college. The electoral college list was extracted from the population register database maintained by EIDA.[1]An application was developed and deployed in all the seven Emirates, where each Ruler Court selected its representative electoral college.

b) **Candidate registration**: The candidates came from the same electoral college list. A clear, standardised, equitable and transparent registration candidate and application review process was essential to maintain the electoral integrity and to ensure that each candidate had an understanding of the requirements and were able to register if qualified. Timely notification of acceptance or rejection, and the right to an appeal if required.

6.3.2 Election Day:

c) **Identity Verification**: Voter verification was carried out using the state-of-the-art smart ID cards issued by the Identity Authority to all the UAE citizens. Voter verification was enabled through the identity toolkit developed by the Identity Authority and integrated with the voting system.

d) **Voting**: Electronic voting machines utilising touch screen monitors for casting votes were deployed. Election servers were deployed at all seven Emirates conducting simultaneous polling electronically in 14 centres across the UAE.

e) **Ballot box**: The e-voting was complemented by a paper print of the e-vote to provide a paper trail and verifiability of the electronic vote count.

6.3.3 Post-Elections:

f) **Vote Count**: Votes were electronically collected from multiple centres, mixed, tallied and results published within minutes of the closure of the voting.

[1] Emirates Identity Authority is a federal government organisation in the UAE established in 2004 to develop and maintain a national identity management infrastructure. Its role involves enrolling all the population in the program by 2013 and issuing them with advanced smart identity cards with their biometrics stored in the chip. The Authority is envisaged to become the primary reference for population demographics data to support strategic planning and decision making in the country. The Authority's role also involves setting up a national validation gateway to support e-government and e-commerce, which all identity verification and authentication transactions will need to go through before the service is availed. Advanced capabilities are possible through the UAE national identity cards, like multi-factor authentication (biometrics, pin, digital certificates), encryption and digital signature.

g) **Reports and Statistics**: From the encrypted databases that provided long-term secure storage, reports were extracted to indicate voter participation, turnout and other vital statistics required by the Government on demand.

A more detailed overview of the finalised business processes implemented in the UAE FNC e-voting system is presented in Annex-2.

6.4. Voters Volumes and Flow in the Voting Centres

Compared to the UAE Elections in 2005, the number of voters for the 2011 FNC elections was 20 times the previous election, 6000 in 2005 and around 130,000 in 2011. This required detailed planning in the areas of site preparation and capacity computation, technical infrastructure development, communication planning, addressing logistical and staff requirements, and the overall specifications of the electronic voting system. The planning phase was fundamental to ensure effective implementation of the electoral process and to encourage and allow a large number of voters to successfully participate in the election.

First, and based on the expected numbers of voters in each Emirate, NEC identified a number of voting centres to accommodate voter capacity in each and every Emirate. See also Figure 10, which depicts the demographics of the FNC electoral college. Next, an analysis using the Erlang model2 based on expected voter turnout, average acceptable waiting time, peak hours and turnout expected during peak hours helped determine the number of voter validation desks and voting booths required at each voting centre.

6.4.1 Calculating capacity

Detailed scientific calculations were carried out to determine the exact number of voting terminals required to cater to the voting needs of the electorate. In a zero waiting time scenario, each voter could be provided with an individual ID verification station and a personal voting station, where the voter could walk in anytime, cast the vote and leave. This would have been a very cost-effective way to meet the voting requirements. The capacity planning and calculation was based on the following constraints:

- The total number of voters was nearly 130,000 spread unevenly across the different Emirates.
- The total number of voting stations identified were 13.
- Voting had to be carried out between 8 am and 8 pm.
- Voters had to be verified for their ID.
- Voters had to be given sufficient time to determine their choices at the voting terminal to select their candidates for casting their votes.

This is where the Queue modelling and traffic calculations resulted in an optimum number of voting terminals spread across different. The calculations followed the Erlang model for traffic calculation. An Erlang is used to describe the total traffic volume in one hour; it is typically used in the Telecommunication industry to calculate the call traffic and maintain the SLAs to the subscribers. The Erlang model is popularly used worldwide for the traffic determination per hour and to ensure that queues are managed optimally.

Figure 11 illustrates the different calculations and models that were used for determining the optimal number of voting terminals.

6.4.2 Vote Anywhere

Vote Anywhere was a feature adopted in the UAE FNC e-voting system to facilitate voting from any voting station without geographic limitations. Technically, a UAE voter could vote in any voting station across the country. However, as per UAE regulations, voters could vote only in their respective Emirates. Thus, the Vote Anywhere feature enabled voters to vote in any of the polling stations in their respective Emirates. For example, voters in the emirate of Abu Dhabi had the option to vote in any of the four voting centres. The use of the UAE national identity card provided higher trust and confidence to enable this feature. The UAE national identity card was the primary identification document that provided authenticated access to the voting system. Once a vote was cast, the ID card chip was updated with a flag of "voted" and it could not be used for voting again. The ID

[2]Erlang is a declarative language for programming concurrent and distributed systems, which was developed by the authors at the Ericsson and Ellemtel Computer Science Laboratories. Agner Krarup Erlang (1878-1929) was a Danish mathematician who developed a theory of stochastic processes in statistical equilibrium - his theories are widely used in the telecommunications industry. Erlang's model primitives provide solutions to problems which are commonly encountered when programming large concurrent real-time systems. The module system allows the structuring of very large programs into conceptually manageable units. Error detection mechanisms allow the construction of fault-tolerant software. Code-loading primitives allow code in a running system to be changed without stopping the system. Erlang has a process-based model of concurrency. Concurrency is explicit and the user can precisely control which computations are performed sequentially and which are performed in parallel. A message passing between processes is asynchronous; that is, the sending process continues as soon as a message has been sent. The only method by which Erlang processes can exchange data is message passing. This results in applications which can easily be distributed - an application written for a uniprocessor can easily be changed to run on a multi processor or network of uniprocessors.

verification system was synchronised across the voting stations in each emirate with the information of the voter verification. The verification system was available in real time across the voting stations in the Emirates. The verification terminals were the starting point for voting, and only when cleared were voters able to proceed to the voting terminal.

6.4.3 Voting Centres Layout

NEC determined an effective voting centre layout for each voting centre to facilitate smooth voter flow during the election day. See also Figure 12. This ensured that only the relevant people had access to relevant areas in the voting centre. This was also supported by a robust technical design set up to ensure accessibility and availability on election day. Figure 13 depicts a network design of a typical voting centre.

On election day, more than 400 volunteering staff were stationed at the voting centres with various roles to support the electronic voting process. Some of these staff were responsible for training voters on the electronic voting system.

6.5Legal Requirements

The e-voting system needed to meet strict security and privacy requirements, and comply with specific constitutional, legal and regulatory contexts related to the electoral rules in the UAE. In general, the following electoral rules were defined:

- Each voting centre to have an Electoral Chief Officer responsible for the voting centre.
- Electoral Board (EB) and Administration Board will be established for each Emirate independently and the voting centres' Electoral Chief Officer will be the principal member.
- The Mixing and Counting process should be initiated and performed in presence of the candidates of the correspondent Emirate for transparency purposes.
- The results of the voting process should be announced and published by the Electoral Chief Officer of each Emirate.

In addition, three legal systems elements were identified and dealt with in detail for the elections. These elements were:

1. Voting systems.
2. Operational instructions.
3. Department of appeals.

The voting systems detailed the type of voting terminals and the technology requirements of the overall voting system. The voting stations, polling booths and connectivity with the central locations were defined. The e-voting infrastructure was laid out. Operational Instructions detailed the voting process. One Voter-One Vote was the defined voting policy. The number of representative seats for each Emirate was defined using proportional representation. Thus, Abu Dhabi and Dubai Emirate had four candidates each to be elected. The Emirates of Sharjah and Ras Al Khaimah had three to be elected, while the Emirates of Ajman, Umm Al Quwain and Fujairah had two each to be elected.

It was also mandated to have a paper ballot printout with the vote cast so that the voting could have a paper ballot trail for count validation. The Department of Appeals allowed appeals for any disputes, or challenges in the post-election phase. It was of paramount importance to ensure the voter and the vote's secrecy. It was thus mandated that the voting system should separate the voter's information from the vote and that there was no way of linking the two.

6.6 Switching from e-Voting to Paper Vote

A contingency procedure was documented and put in place to address any requirement to switch from e-voting to manual paper voting. The procedure was required to be authorised by electoral authorities. In this case, the steps to follow were:

- The voting centre officer should announce the situation to the candidates, as well as the voters and the public witnessing the event.
- The voting centre officer should also announce that the *vote anywhere* option is disabled (for the voting centre) and only a voter assigned to the voting centre will be authorised to cast the vote.[3]

[3]When authorised, the 'voting anywhere' system was to be procedurally disabled owing to the non-availability of the e-voting system. Keeping this contingency in mind, voters were mapped to the voting stations nearest to their residences. Thus, for example, all Al Ain-based voters were pre-mapped to the voting station in Al Ain, while voters in Jumeira city were mapped to the voting station in Dubai World Trade Centre. Poll workers were trained to refer to the vote's list with this mapping, and direct the voters to their respective voting stations in such a contingent situation.

- Assistant Technicians will verify that e-votes cast were synchronised with central server.
- The voting centre officer will authorise the procedure and technicians will shutdown the e-voting solution.
- Poll-workers receive the pre-printed clean ballot papers to be handed to the voters.
- Poll-workers also receive the authorised list of voters of the voting centre (from the poll-book application) including the information of the voter who had already cast the vote.
- Poll-workers will resume the voting process, providing to the voter the paper ballot instead of the ID credential to vote.

See also Figure 14.

6.7 Security Features in the System

The analysis conducted by the technical committee concluded that the overall security of the e-voting system is dependent on the level of protection provided by the operational processes put in place, rather than the security features of the system itself. This is also in compliance with the findings of Hisamitsu and Takeda (2007), who stated that the security issues in e-voting systems arise from lack of protection mechanisms and procedures on tabulation machines. Each and every one of the almost 800 voting stations and 300 pool-workers laptops were hardened i.e. the basic software was restricted and their connectivity features limited so they could only be used for the election.

Overall, the computerised e-voting system was required to meet all the security aspects of manual voting. The committee defined the following measures to be implemented to support the overall security of the system.

6.7.1 Software Certification

- The e-voting software itself was an international commercial e-voting solution that was based on proprietary source codes. The e-voting system was required to be certified by an international body. The core e-Voting Solution was certified by an independent international body following EU guidelines, namely the Austrian Centre for Secure Information Technology (A-Sit), an independent renowned certification Authority appointed by the Federal Ministry of Science and Research to certify the security of the software. The audit was carried out applying the e-voting standards of the European council as well as analysing the security architecture and source code of the e-voting software in accordance with the Austrian students' law. The used software development processes and methodologies were audited against ISO/IEC 15408. Certification process guaranteed that the machines and software were reliable and secure.

6.7.2 Security of voting centre equipment and communication

- Network segregation was used for the local networks at the voting sites, including networks for voting terminals and poll-books, database network, and external network connection.
- All servers use local firewalls.
- All operational machines (laptops and voting terminals) were locked to allow only authorised changes to the software installed on these machines.

6.7.3 Data Security

- SSL connections were established between voting terminals and application servers.
- Voting options were encrypted at the voting terminal with a digital envelope using the Election Public Key.
- The digital envelopes containing the voting options were digitally signed using anonymous digital certificates.

6.7.4 Voter Authentication

- Voters were authenticated using their biometrics stored in the national electronic ID cards.
- A secure flag was recorded on the ID card to indicate that the voter had been verified and was then allowed to vote in the same site.
- The verified card could then be used to vote.
- At the voting station, a digital certificate was used to authenticate the voter and to secure the voting session.
- The digital certificate was also used to encrypt the electronic vote.
- Once the vote was cast in the voting system, the card was flagged to prevent the voter from accessing the voting system again.

6.7.5Voter Anonymity

- The encrypted votes were digitally signed with anonymous digital certificates.
- The signed votes were decrypted only using the election private key, which was constructed from the individual keys of the electoral board members. This step was done after the voting was complete in order to start the counting.
- During the mixing, the system broke any correlation between the encryption envelope and the vote content. The outcome of this step was that the contents of all votes were cast into the system during the voting, with no links whatsoever between each vote and the identity of the voter.
- Temporal or residual information managed by the voting applications (e.g. cookies or temporal records) were destroyed after the vote casting, removing any possible trace containing the voter information or vote selections.

6.8 Pilot Test

The e-voting system was piloted two weeks prior to election day. More than 600 volunteering staff of EIDA participated in the testing of the system. Although no major technical issues were identified, many of the reported issues were related to usability and overall organisation. Much attention was needed to be given to the training of support staff on election day.

Meticulous planning went into the pilot testing. All systems were setup in the actual voting site in Dubai. This was a mock system working in actual voting conditions. The pilot itself was a culmination of the factory acceptance tests, followed by detailed user acceptance tests (UAT) conducted on the e-voting systems. The test scripts used for the UAT set the tone for the pilot testing. The pilot thus was the actual dry run prior to the elections.

The dry run served two purposes. The first was to test the resilience of the e-voting system, while the second was to ensure that human resources were trained and acquainted with the voting systems for the election day. The scope of dry run was also to test:

1. The complete e-voting solution required to run the voting process on election day with the required IT Infrastructure; and
2. The actual voting process as prescribed for UAE elections 2011.

Dubai was chosen as the location for the dry run. The identified voting centre at the Dubai World Trade Centre was setup with the coordination and cooperation from the DWTC team.

Table 6 outlines some additional elements that took place during the pilot test.

6.9 The Election Day

Early preparation activities started a few days in advance with election system configuration and final setup for each Emirate. This involved updating the e-voting system in each Emirate with voters and candidates list, configuring the election start and end date/time for elections in each of the seven Emirate, etc. The electoral and administration board in each Emirate was the responsible team to authorise the beginning and the end of the election in their Emirates.

The election commenced on September 24th, 2011 at 8 am. Election day activities started with a team briefing by the voting centre manager, after which designated and trained staff started the procedure of booting up the voting terminals and initiated the process of voter identification applications. See Figure 15. Technical and support staff were present at the voting centres to assist voting centre staff in electronic voting process related matters.

Following were the primary set of rules governing voting procedures related to what happened at polling centres. See also Figure 16. Voters arriving at the voting centre were:

1. Guided by receptionists to training areas. Separate group and individual training areas in the voting centres were setup to familiarise voters and prepare them for the voting process.
2. Voters were validated at ID verification desks. Individuals arriving to vote were identified using their ID cards and validated against the electoral roll. Only valid voters were allowed to proceed to the voting area.
3. Valid voters cast their votes electronically at the voting terminals. Voters used their ID cards or smart cards prepared for voting to cast their electronic vote. The system only allowed a voter to vote once. Once the electronic vote was cast, a printed copy of the ballot was printed.
4. Voters were instructed to fold and insert the ballot copy in one of the ballot boxes and then exit the voting centre.

As mentioned previously, each voting centre had its own local servers to maintain the record of votes cast during the day. For those Emirates that had more than one voting centre, ballots were synchronized among voting centres within the same Emirate to maintain a view of participation within the Emirate. Aggregated participation

information of each Emirate was sent to the main Abu Dhabi site periodically to display aggregated participation information. The whole voting process throughout the country was monitored by the higher commission members at the operations management centre, which was set up to handle the technical and organisational issues that arose.

Ballot counting started when the election ended at 8:00 pm and the electoral board of the Emirate authorised the process. An additional hour was granted in the Emirates of Abu Dhabi due to growing numbers of voters in the last hours. The results of each Emirate were announced in the main voting centre of the Emirate. Overall, more than 35 thousand citizens participated in casting their ballots electronically. Figure 17 depicts the survey results conducted by some international research companies that outline the overall perception of citizens around FNC elections.

7. Success Factors

From a technical perspective, the use of advanced cryptographic protocols enabled all types of election processes to be carried out in a completely secure, transparent and auditable manner. The solution accorded the highest levels of security, in terms of voters' "privacy, ballot box integrity, and voter-verifiability".

The key success factors that have led to the success of the FNC e-voting experience were related to "structure and readiness", which can be summarised as follows:

a) Organisation Structure: the structure played a key role in getting together many government departments to work cooperatively to support the FNC elections. The structure included more than 100 officials representing different government and public sector organisations, in addition to more than 900 volunteering staff who supported the 14 voting centres throughout the country.
b) Site readiness: a comprehensive detailed plan (Go-live plan) was defined to govern the prerequisite activities for the elections day. Great attention was given to election site preparation.
a) System readiness: the go-live plan mentioned above included activities related to the voting system deployment in the voting centres. These activities included thorough testing of the system after deployment in the voting centres to ensure all equipment was working properly and to test the sites' connectivity.
c) Staff readiness: this was achieved by the training and the dry run (pilot) simulation. A comprehensive training plan was defined and implemented to cover these activities. Staff training in the new methods of voting to a level good enough to provide on-sight voter education and process knowledge-gathering provided valuable input to the election day.
d) Communication: This was recognised to be the most critical success factor. The key to strong communication was the ability to define the process and timescales at the outset. There was constant communication at every level of the election planning and execution process with the stakeholders through public meetings, workshops, local conferences, etc.
e) Social Media:[4]The use of social media and its social networks supported the success of the FNC elections, as it turned communication into an interactive dialogue between the NEC commission, local communities and individuals. Social media played an important role in widening accessibility and scalability of communications.

In addition to the above critical success factors, the application of the UAE population register and smart identity card was considered to have added significant contribution to the overall success of the NFC elections.

7.1 Using the UAE Population Register in the Voting System

1. The UAE National Register was used to extract the list of the electoral colleges. The Register is the most accurate and unique population database in the country, as it depends on advanced technologies to link the biographical information to the individuals, namely facial and fingerprint biometrics.
2. The voters' list was uploaded to the voting system before the elections. This list was used to verify voters and ensure only legitimate voters were using the voting terminals to cast their electronic votes.
3. In addition to the voters list, the national register was also used to extract the list of candidates, which was also uploaded to the voting system.
4. General voter information available on the national register was also used in the voters' list. The information included was age, gender, profession, Emirate, etc. This information was used by the voting

[4]Social media has changed the way people connect, discover and share information. Social media is the technology that connects people, whether it is to share content or just to chat. Kaplan and Haenlein (2010) define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0 (a website that doesn't just give you information, but interacts with you while giving you that information), and that allow the creation and exchange of user-generated content".

system to provide statistical reports and dashboards during and after the elections.

5. The mobile numbers available in the national register were also useful to send awareness SMS messages to the voters before and on election day.

7.2 Using the ID Card for Voting

The UAE biometric-based national identity card was an important component which made secured e-voting possible. The importance of the electronic ID card is summarised by the following points:

1. The card was used to verify the identity of voters. Biometric verification was used in the verification process, and in cases when physical verification using picture comparison was not possible.
2. The card was also used to ensure that only verified voters could access the voting terminals.
3. After the vote was cast in the system, the card and e-voting system were flagged to ensure the voter could not use his card to vote again.
4. In the above process, vote buying was not possible, as was the case in other voting systems where electronic ID cards were not used. This was due to the fact that only the card owner could use his/her card to vote after being verified.

8. Lessons learnt

The UAE e-voting system was conceived, designed and deployed, and worked exceptionally well albeit with some glitches and operational issues. Although it did not pose any serious risk to the overall and final election results, a few of the identified issues need to be heeded by election officials during planning and execution phases.

Some of the major challenges faced on election day were:

1. Some of the electronic voting systems developed unanticipated screen freezes, leaving voters wondering whether their ballots had been properly recorded. Despite this situation, voters were able to try to cast their ballot electronically again, but they got error messages informing them that they have already voted or they were not allowed to vote again. On-site support was provided to check whether the ballot was casted correctly or not.
2. Some printers went into sleep mode, which needed supervisor intervention to print the votes cast. Some printers were on the default settings to go on the sleep mode if unattended for a few minutes. The technical staff needed to visit each and every printer to change the default settings. With these printers in sleep mode, the ballots were not successfully printed but they were stored electronically. A reprinting feature was accessible with a specific password, although it seemed to be unknown by some participants. This feature is further described at Annex 2.
3. Some voters by-passed the voter identification and went straight to the voting terminals only to find that the system did not allow them to cast their votes, leading to confusion among the voters.
4. During the mixing and tallying period, the data synchronisation between two major polling stations stalled and it took some time for the data synchronisation to be completed. This delayed the announcement of the election results in the Emirate of Abu Dhabi for about an hour. The issue was related to the MPLS data link between Abu Dhabi and Al Ain that had some problems and the ballot synchronisation speed was slow. This affected the mixing process, as it could not be executed until all the information was synchronised. This was not a mixing problem, but a data-readiness problem i.e., the pre-requisite of the mixing process was to have all the information synchronised.
5. Some voters' identity could not be verified when they used the national ID cards; thus, they were issued with white smart cards in the voting centres to enable them cast their votes. This scenario was defined as a fallback scenario for voters whose identity card was damaged and their chip was not readable. This scenario is further described at Annex 2. Thanks to having this scenario defined and implemented, all voters were able to cast their ballots. A similar verification process was executed with these voters.

Serious as they seem, all these challenges were overcome quickly due to the contingency measures put in place in the e-voting system and the overall procedures. For every issue reported, trained technical staff identified the root cause and set in motion the contingency plans to enable restoration of the voting process.

The local area network was quickly brought up and the voting system was restored for casting votes where the screen freezes were reported. The screen freeze was attributed to the inability of the LAN to load the voting applet on the voting terminals from the server.

Specifically during the first three hours, management and technical staff were on the move within the voting centres to ensure that the printers were kept active throughout the voting period. Stricter controls were enforced ensuring that the voters did not approach the voting terminals without their identity being verified, thus enabling a smooth voting process. The network was fine-tuned to ensure data synchronisation between the affected sites.

As indicated above, and where the national ID card could not be verified, authorised voterswere provided

with "White Cards" enabling them to cast their votes on the e-voting terminals. Interestingly, the majority of those people who had shown up on election day and reported that their national ID cards did not work, were later recognised as not being in the electoral college in the first place. As a result, those individuals needed to be dealt with very carefully.

Another important lesson learnt related to the fact that the UAE e-voting system only printed voters' copies that were put in the ballot boxes by the voters. No separate receipts were printed for voters' own records. Some of the voters expressed concerns and wondered if their votes were actually counted. It is, therefore, recommended that, for the following elections, NEC should put in place kiosk machines with an application to allow voters to check whether their votes were counted after the mixing stage. Instead of a separate receipt issuance, national identity cards could be used as a token to be inserted into such kiosk machines for electronic verification. This step is envisaged to enhance voters' confidence and trust levels.

Taken as a whole, these contingency measures, combined with on the ground leadership from the top management (Higher Election Commission members),ensured a successful culmination of this ambitious project of e-voting in the UAE. The following would stand out as the main highlights of the UAE FNC elections exercise:

- Successful completion of the elections using e-voting
- All voting results for winners announced the same day and within hours of the closing of voting
- Successful deployment of national ID card for ID verification
- Tremendous coordination effort in organising, deploying and running the e-voting system, involving many entities and individuals across the country. This more than amply demonstrates the leadership qualities and the organising abilities of the project management team and the project sponsoring committee, i.e. the NEC.

The success of this e-voting system has laid the foundation for the UAE to step forward towards full i-voting system deployment. The UAE now has all the technological and technical components required to make this a reality. These are as follows:

1. Proven national ID card that carries the digital certificates from the Population PKI that should enable identification, validation, authentication, digital signing and encryption.
2. Proven e-voting system that was designed based on browser-based voting on PCs. The voting terminals were designed as kiosks with touch screen PCs embedded in the kiosks, with ID Card readers and biometric units.
3. Proven e-voting system that has been successfully deployed and fully integrated with the national ID card as a verification tool.
4. Proven nation-wide interconnectivity and bandwidth that enables remote voting.
5. Robust e-voting practice and process that enables secure and reliable voting remotely.
6. A legal system that has had experience with using the national ID cards as the primary token for identification.

9. Conclusion

As computing technology and security technologies has evolved, so too has the adoption of e-voting technologies for conducting national elections evolved. Technologically advanced countries and countries with electoral maturity have set the pace for the e-voting adoption. Although countries have had different experiences with electronic voting systems, there seems to be a consensus among governments on the importance and the positive impact of electronic voting systems on the overall election systems. The literature identified numerous advantages of electronic voting systems over traditional paper ballot voting, namely convenience, usability, simplicity, cost savings, reliability, etc. These factors explain to some extent the underlying reasons behind the growing interest of governments to deploy electronic voting systems.

In this article, we attempted to provide an overview of elections and e-voting systems. We covered the existing literature to review the critical points of current knowledge, including substantive findings and contributions to the particular topic of e-voting. The article then moved to provide an overview of the UAE FNC elections in detail. The presented research content is considered to be of great support to similar endeavours, specifically as countries worldwide are showing greater interest in the application of e-voting systems.

In general, the FNC 2011 elections were seen as one of the most successful initiatives of the year in the UAE. The e-voting system was considered by the government to be a major improvement to the manual voting process in terms of:

- Integrity: The e-voting system is an extremely secure system that cannot be tampered with by anyone, including system administrators.

- Speed: Vote counting and results announcement was done based on the electronic votes in the system within less than an hour after closing the voting centres.
- Transparency: The entire voting process was observed by the candidates and their representatives as well as the media. The system was open for audit by external and internal auditors. Vote counting was done automatically and entirely by the system. Preliminary results from the system were presented in each of the 14 voting centres that promoted transparency, and for the candidates to see them before the official announcement of results.

The voting procedures announced through different media channels played a major role to encourage participation and turnout. The use of the government-issued advanced smart national identity cards to identify the voters and candidates acted as an effective enabler of the e-voting system. By and large, the automated e-voting system enabled smooth and fast elections across the seven Emirates to be conducted and closed on the same day.

8.1 Future Work

Research in the field of e-voting is an important factor in improving the overall knowledge, where it can provide much valuable information from sharing the results of different pilots and experiments in countries worldwide. Such a range of experience provides a wealth of practical information, knowledge and inputs. The content of the research and the lessons learnt from the deployment of the e-voting in the FNC election in the UAE can serve as a set of valuable guidelines for the future design and deployment of e-voting systems in Arab countries and worldwide.

Indeed, the case study approach adopted in this research has its limitations; generalisability is not possible due to the information source being from a single case. However, it needs to be heeded that the UAE e-voting system design and procedures from technical, legal, management and other dimensions were benchmarked with other implementations in other countries. This reduces and addresses the concerns over case study limitations.

The government of the UAE is in the process of trialing an internet-based e-voting system. The application will be available for deployment for any election requirement in the public sector. The system will rely greatly on the smart identity card capabilities for strong authentication. The public key cryptography will form the foundation on which secure communications will be established. The government trusts that biometrics, smart cards, and national cryptography will, altogether, provide strong mechanisms to protect the integrity of voter registration information and overall elections process.

In our opinion, the use of government-issued smart cards adds a new dimension of security and contributes to the overall trust and confidence of the public. More research is inevitable, such as the Internet, in order to explore how such cards could support the development of more secure electronic voting over public networks.

References

Alexander, K. (2001), “Ten Things I Want People to Know About Voting Technology”, Presented to the *Democracy Online Project’s National Task Force*, National Press Club, Washington, D. C., January 18, 2001.

B. Schoenmakers. (1999), “A simple publicly verifiable secret sharing scheme and its application to electronic voting”. In Advances in Cryptology-CRYPTO ‘99, Vol. 1666 of Lecture Notes in *Computer Science*, pp. 148-164, Berlin. Springer-Verlag.

Barr, C.W. (2006) Security Of Electronic Voting Is Condemned, Washington Post. *http://www.washingtonpost.com/wp-dyn/content/article/2006/11/30/AR2006113001637.html* Accessed on 12/03/12.

Bonsor, K. and Strickland, J. (2007), "How E-voting Work: The Psychology of Electronic Voting." *http://people.howstuffworks.com/e-voting5.htm* Accessed on 12/03/12.

Bonsor, K. and Strickland, J. (2011) How E-voting Works. http://www.howstuffworks.com/e-voting.htm

Caltech-MIT (2001), "A Preliminary Assessment of the Reliability of Existing Voting Equipment," The Caltech-MIT Voting Technology Project, March 30, 2001. Available at *http://www.vote.caltech.edu/Reports/index.html* Accessed on 12/03/12.

Chaum, D. (2004), "Secret-Ballot Receipts: True Voter-Verifiable Elections." *IEEE Security and Privacy*, **2**(1): 38–47.

Chiang, L. (2009), "Trust and security in the e-voting system," *International Journal of Electronic Government*, **6**(4), pp. 343-360.

CIVTF (2000), “A Report on the Feasibility of Internet Voting,” California Internet Voting Task Force, *http://www.sos.ca.gov/elections/ivote/final_report.pdf* Accessed on 11/04/12.

Clausen, D., Puryear, D., & Rodriguez, A. (2000), "Secure voting using disconnected distributed polling devices." Palo Alto. CA: Standford University. *http://www-cs-students.stanford.edu/~dclausen/voting/cs444n_voting_report.pdf* Accessed on 10/01/12.

Crane, R., Keller, A. Dechert, A., Cherlin, E. and Mertz, D. (2005), "A Deeper Look: Rebutting Shamos on

e-Voting," *http://www.verifiedvoting.org/downloa-ds/shamos-rebuttal.pdf* Accessed on 12/03/12.
Cranor, L.F. (2000), "Voting After Florida: No Easy Answers." *http://lorrie.cranor.org/voting/essay.html* Accessed on 12/03/12.
Done, R. S. (2002), "Internet Voting: Bringing Elections to the Desktop," Research Report, PricewaterhouseCoopers Endowment for the Business of Government, 2002, *http://www.endowment.pwcglobal.com/pdfs/Done_Report.pdf* Accessed on 12/03/12.
e-Gov Monitor (2003), "Does the UK need e-voting?." *http://www.egovmonitor.com/features/evoting2003.html* Accessed on 12/03/12.
Britannica (2012), "Encyclpoedia Britanica." *http://www.britannica.com* Accessed on 01/01/12.
E-Poll (2012) *http://www.e-poll-project.net* Accessed on 01/01/12.
González, J.F. and Brambila, S.B.G. (2012), "Secure Architectures for a Three-Stage Polling Place Electronic Voting System," *Computación y Sistemas* **16**(1), pp 43-52.
Hargrove, T. (2004), "Widespread voting woes foil democratic process. Old equipment, faulty accounting methods fail to tabulate many votes. *The Detroit News*.
Hisamitsu, H. and Takeda, K. (2007), "The security analysis of e-voting in Japan", Alkassar, A. and Volkamer, M. (Eds), "E-Voting and Identity," Proceedings of *VOTE-ID'07 1st international conference on E-voting and identity*. Springer-Verlag Berlin Heidelberg, New York, pp.99-110.
Hoffman, LJ. (2004), "Internet Voting: Will it Spur or Corrupt Democracy?," Technical Report, Computer Science Department, The George Washington University, Washington, D. C. *http://www.cfp2000.org/papers/hoffman2.pdf* Accessed on 01/01/12.
Hout, M, Mangles, L, Carlson, J. and Best, R. (2004), The Effect of Electronic Voting Machines on Change in Support for Bush in the 2004 Florida Elections. *http://ucdata.berkeley.edu/new_web/VOTE2004/election04_WPwappendices.pdf* Accessed on 01/01/12.
IDEA (2011), "Introducing Electronic Voting: Essential Considerations," Policy Paper, The International Institute for Democracy and Electoral Assistance. *http://www.agora-parl.org/sites/default/files/e-voting_idea.pdf* Accessed on 01/01/12.
Ikonomopoulos, S.; Lambrinoudakis, C.; Gritzalis, D.; Kokolakis, S.; Vassiliou, K. (2002), "Functional Requirements for a Secure Electronic Voting System," , in Proceedings of the *17th IFIP International Conference on Information Security*, pp. 507-520, Egypt, Kluwer Academic Publishers. *http://www.instore.gr/evote/evote_end/htm/3pub-lic/doc3/public/aegean/paper4.pdf* Accessed on 01/01/12.
IPI (2001), "Report of the National Workshop on Internet Voting: Issues and Research Agenda," Internet Policy Institute, available at *http://verifiedvoting.org/downloads/NSFInternetVotingReport.pdf* Accessed on 01/01/12.
Jones, D.W. (2001), "Evaluating Voting Technology," Testimony before the United States Civil Rights Commission, Tallahassee, Florida. *http://homepage.cs.uiowa.edu/~jones/voting/ArizonaDist20.pdf* Accessed on 01/01/12.
Kaplan, Andreas M.; Michael Haenlein (2010), "Users of the world, unite! The challenges and opportunities of Social Media". *Business Horizons* **53**(1): 59–68.
Klein, P. (1995), "An Untraceable, Universally Verifiable Voting Scheme," Seminar in Cryptology, December 12, 1995.
Kosmopoulos, A. (2004), "Aspects of Regulatory and Legal Implications on e-Voting," *Lecture Notes in Computer Science*, **3289**, pp. 589-600.
Law, G. (2002) "Britain back on e-voting track. UK city council begins smartcard e-government plan." *PC Advisor* Thursday, 25 April 2002.
Levy, S. (2004), "Ballot Boxes Go High Tech." *MSNBC Newsweek*.
Liptrott, M (2006), "e-Voting in the UK: a Work in Progress," *The Electronic Journal of e-Government*, **4**(2), pp 71-78.
Manjoo, F. (2002), "Voting into the void New," *Salon*, 5 November, *http://www.salon.com/2002/11/05/voting_machines_2/* Accessed on 01/01/12.
Manjoo, F. (2003a), "Another case of electronic vote-tampering?" *Salon*, 29 September, *http://www.salon.com/tech/feature/2003/09/29/voting_machine_standards* Accessed on 01/01/12.
Manjoo, F. (2003b), "An open invitation to election fraud." *Salon*, 23 September, http://www.salon.com/tech/feature/2003/09/23/bev_harris Accessed on 01/01/12.
Mercuri, R. (1993), "The Business of Elections," CFP'93, *http://www.cpsr.org/conferences/cfp93/mercuri.html* Accessed on 01/01/12.
Mercuri, R. (2002), "A Better Ballot Box?", *IEEE Spectrum*, **39**(10), pp. 46-50.
Millar, S. (2002), "Don't trust computers with e-votes, warns expert." *The Guardian*, Thursday October 17. *http://www.guardian.co.uk/politics/2002/oct/17/uk.internet* Accessed on 01/01/12.
Neumann, P.G. (1993), "Security Criteria for Electronic Voting," *16th National Computer Security Conference*,

Baltimore, Maryland, September 20-23.
NIST (2006), "Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC," The National Institute of Standards and Technology (NIST). *http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf* Accessed on 01/01/12.
NIST (2008), "A Threat Analysis on UOCAVA Voting Systems," NISTIR 7551, The National Institute of Standards and Technology (NIST). http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf Accessed on 01/01/12.
NIST (2011), "Security Considerations for Remote Electronic UOCAVA Voting," NISTIR 7770, The National Institute of Standards and Technology (NIST). http://www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf Accessed on 01/01/12.
O'Donnell, P. (2004), "Broken Machine Politics." *Wired Magazine*, January 2004. *http://www.wired.com/wired/archive/12.01/evote_pr.html* Accessed on 01/01/12.
Oostveen, A. and P.van den Besselaar (2004), "Security as Belief. User's Perceptions on the Security of Electronic Voting Systems." In: Prosser, A. and Krimmer, R. (eds.) "Electronic Voting in Europe: Technology, Law, Politics and Society." *Lecture Notes in Informatics*. P-47, pp.73-82. Bonn: Gesellschaft für Informatik. *http://www.social-informatics.net/ESF2004.pdf* Accessed on 01/01/12.
Oostveen, A. and van den Besselaar, P. (2004), "Ask No Questions and Be Told No Lies. Security of computer-based voting systems: trust and perceptions." In Gattiker, U.E. (Ed.), *EICAR 2004 Conference*. Copenhagen: EICAR e.V.
Oostveen, A. and van den Besselaar, P. (2004) Internet voting technologies and civic participation, the users perspective. Javnost / The Public Vol. XI [2004], No.1, p61-78. ISSN 1318 - 3222.
Oostveen, A., van den Besselaar, P. (2004), "E-democracy, Trust and Social Identity: Experiments with E-voting technologies."
Oostveen, A., Van den Besselaar (2005), "The Effects of Voting Technologies on Voting Behaviour: Issues of Trust and Social Identity. In: *Social Science Computer Review,*.**23**(3), Fall 2005, pp.304-311, Sage Publications.
Oostveen, A., van den Besselaar, P. (2006), "Non-Technical Risks of Remote Electronic Voting." In: Ari-Veikko Anttiroiko and Mattia Malkia (eds.), The Encyclopedia of Digital Government. Idea Group Inc. pp 502-507.
Phillips, D. and von Spakovsky, H. (2001), "Gauging the risks of internet elections." *Communications of the ACM*, **44**(1), pp. 73-85.
Pratchett, L. and M. Wingfield (2004), "Electronic voting in the United Kingdom. Lessons and limitations from the UK Experience" in: Kersting, N. and Baldersheim, H. (eds.) *Electronic Voting and Democracy. A Comparative Analysis*. London: Palgrave Macmillan.
Prosser A. and R. Krimmer (eds.) (2004), "Electronic Voting in Europe: Technology, Law, Politics and Society." *Lecture Notes in Informatics*, P-47, pp.73-82. Bonn: Gesellschaft für Informatik.
Quesenbery, W. (2003), "Starting from People: Usability and User-Centred Design in Voting Systems." NIST Symposium on Building Trust and Confidence in Voting Systems. *http://www.nist.gov/itl/vote/upload/6-Quesenbery.pdf* Accessed on 01/01/12.
Cramer, R., Franklin, M., Schoenmakers, B. and Yung, M. (1996), "Multi-authority secret ballot elections with linear work". In: *Advances in Cryptology-EUROCRYPT '96*, Lecture Notes in Computer Science **1070**, pp. 72-83, Berlin: Springer-Verlag.
Rapoport, R.N. (1970), "Three Dilemmas in Action Research," *Human Relations*, **23**, 499-513.
Rivest, R.L. (2004), "Electronic voting, technical report," Laboratory for Computer Science, Massachusetts Institute of Technology. *http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting.pdf* Accessed on 01/01/12.
Rubin, A.D. (2002), "Security Considerations for Remote Electronic Voting," *Communications of the ACM*, **45**(12), pp.39-44.
Salem, F. (2007), "Enhancing Trust in e-Voting through Knowledge Management: The Case of the UAE," Dubai School of Government. United Nations Public Administration Network. *http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan026090.pdf* Accessed on 01/01/12.
Saltman, R.G. (1975), "Effective use of computing technology in vote-tallying," The National Institute of Standards and Technology (NIST). *http://csrc.nist.gov/publications/nistpubs/NBS_SP_500-30.pdf* Accessed on 01/01/12.
Schneier, Bruce (2004), "What's wrong with electronic voting machines?," openDemocracy *http://www.opendemocracy.net/media-voting/article_2213.jsp* Accessed on 01/01/12.
Wolchok, S., Wustrow, E. Isabel, C. and Halderman, J.A. (2012), "Attacking the Washington, D.C. Internet Voting System," In: *Proceedings of the 16th Conference on Financial Cryptography & Data Security*. *https://jhalderm.com/pub/papers/dcvoting-fc12.pdf* Accessed on 01/01/12.
Shamos, M.I. (1993), "Electronic Voting – Evaluating the Threat," International Conference on Computers, Freedom, and Privacy, Burlingame, California.

Susman, G.L. and Evered, R.D. (1978), "An Assessment of the Scientific Merits of Action Research," *Administrative Sciences Quarterly*, **23**(4), pp.582-603.
UAE NEC (2011), UAE National Election Commission. *http://www.uaenec.ae* Accessed on 01/01/12.
UK POST (2001), "Online Voting," postnote – a publication of the U. K. Parliamentary Office of Science and Technology. *http://www.parliament.uk/briefing-papers/POST-PN-155.pdf* Accessed on 01/01/12.
Van den Besselaar, P. and A. Oostveen (2003), "E-voting is not neutral!" In: *Lecture Notes in Informatics* **P35**, pp. 218-221.
Van den Besselaar, P. and A. Oostveen (2004), "Media effects in voting and polling: e-democracy, trust and social identity." In: *Proceeding of the 2004 ICA Conference 'Communication in the Public Interest*, New Orleans.*http://citation.allacademic.com/meta/p_mla_apa_research_citation/1/1/3/0/1/pages113010/p113010-1.php* Accessed on 01/01/12.
Volkamer, M. (2009), *Evaluation of Electronic Voting*. Berlin: Springer-Verlag.
Waddington, D. (1994), "Participant Observation," in: Cassell, C. and Symon, G. (eds.) *Qualitative Methods in Organizational Research - A Practical Guide*. London: Sage.
Walsham, G. (1993), *Interpreting Information Systems in Organizations*. Chichester: John Wiley & Sons.
Windley, P.J. (2005), "eVoting, Extreme Democracy," In: Lebkowsky, J. and Ratcliffe, M. (eds.) Extreme Democracy. Internet/Media Strategies, Inc. pp, 132-138. http://www.extremedemocracy.com/chapters/Chapter%2011-Windley.pdf Accessed on 01/01/12.
Xenakis, A. and Macintosh A. (2006), "A generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process," In: Krimmer, R. (Ed.) "Electronic Voting 2006," *Lecture Notes in Informatics*. 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting.CC. August, 2nd– 4th in Castle Hofen, Bregenz, Austria.
http://www.e-voting.cc/wp-content/uploads/Proceedings%202006/5.1.Xenakis_Macintosh_BPR_in_E-Voting_119-130.pdf Accessed on 01/01/12.
Zetter, K. (2003), "E-Vote Firms Seek Voter Approval." *Wired News*. *http://www.wired.com/news/evote/0,2645,60864,00.html* Accessed on 01/01/12.

Dr. Ali M. Al-Khouri is the Director General (Under Secretary) of Emirates Identity Authority; a federal government organisation established in 2004 to rollout and manage the national identity management infrastructure program in the United Arab Emirates. He has been involved in the UAE national identity card since its early conceptual phases during his work with the Ministry of Interior. He has also been involved in many other strategic government initiatives in the past 22 years of his experience in the government sector. He holds an engineering doctorate degree in strategic and large scale programs management from Warwick University, UK; Masters Degree (M.Sc.) in Information Management from Lancaster University, UK; and a Bachelors Degree (B.Sc., Hons.) from Manchester University, UK. He is also a member in several academic and professional institutions. He is an active researcher in the field of advanced technologies implementation in government sector, and the approaches to reinventing governments and revolutionising public sector services and electronic business. He has published more than 50 research articles in various areas of applications in the past 10 years.

Figure 1: Conventional ballot-based voting system

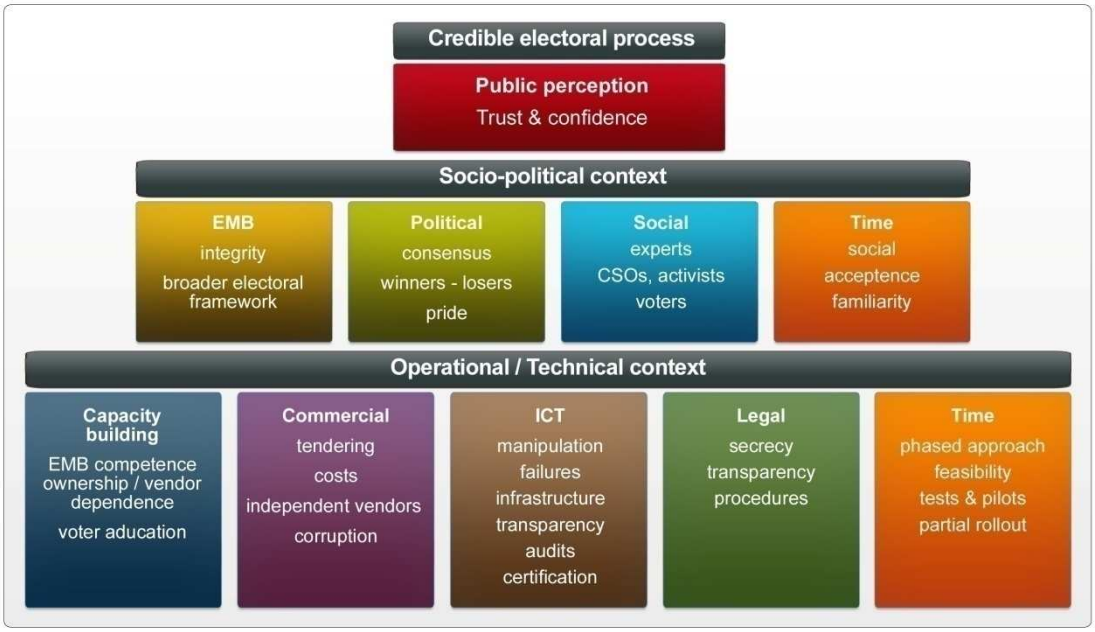


Figure 2: The pyramid of trust

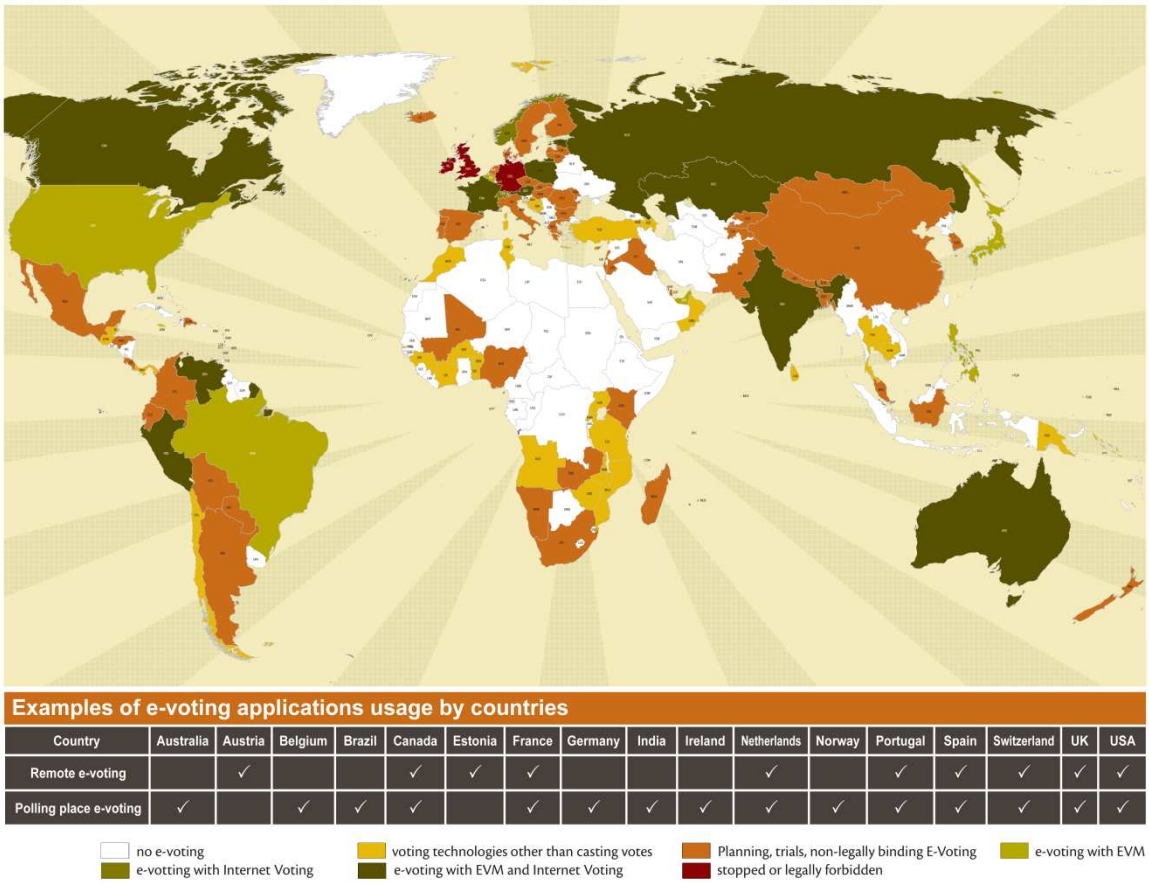


Figure 3: e-voting around the world (source e-Voting.cc)

Figure 4: 2006 vs. 2011 FNC elections

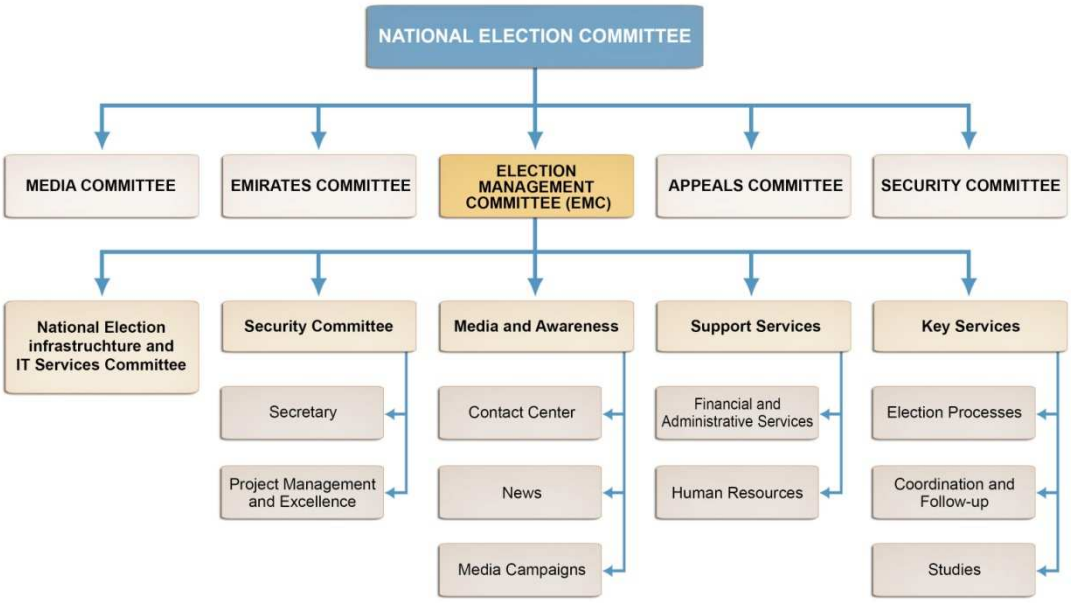


Figure 5: National Election Commission Structure

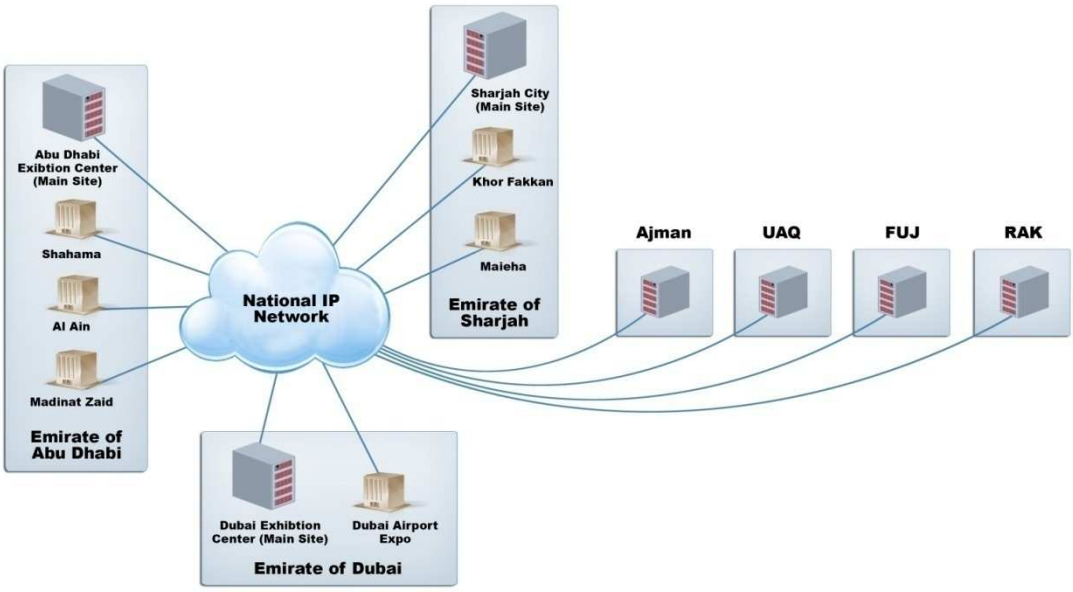


Figure 6: FNC e-voting system architecture

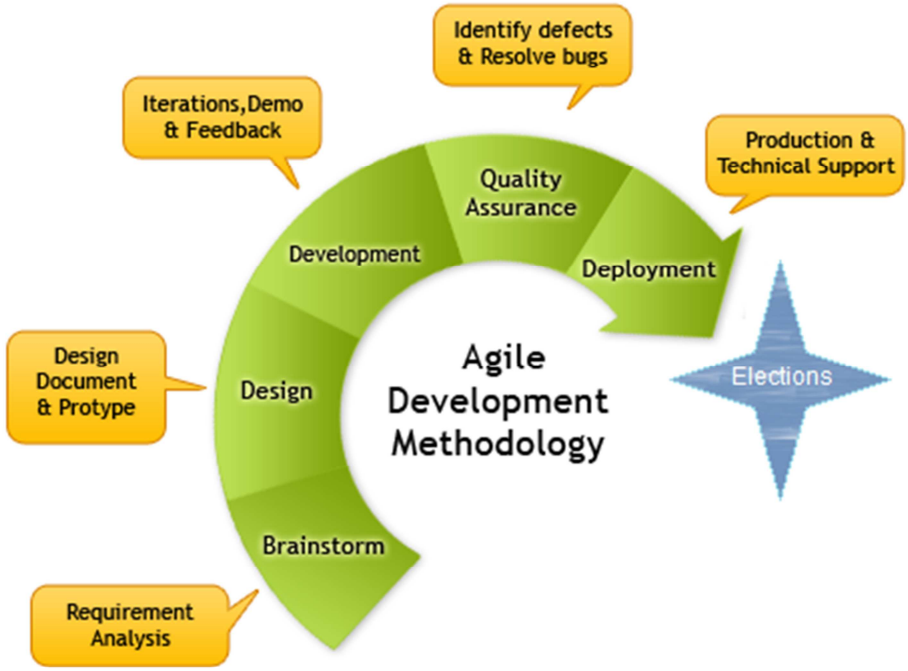


Figure 7:UAE e-voting deployment methodology

Back Sheet Filled sample vote sheet Front Sheet

Figure 8: Approved design of the FNC ballot paper

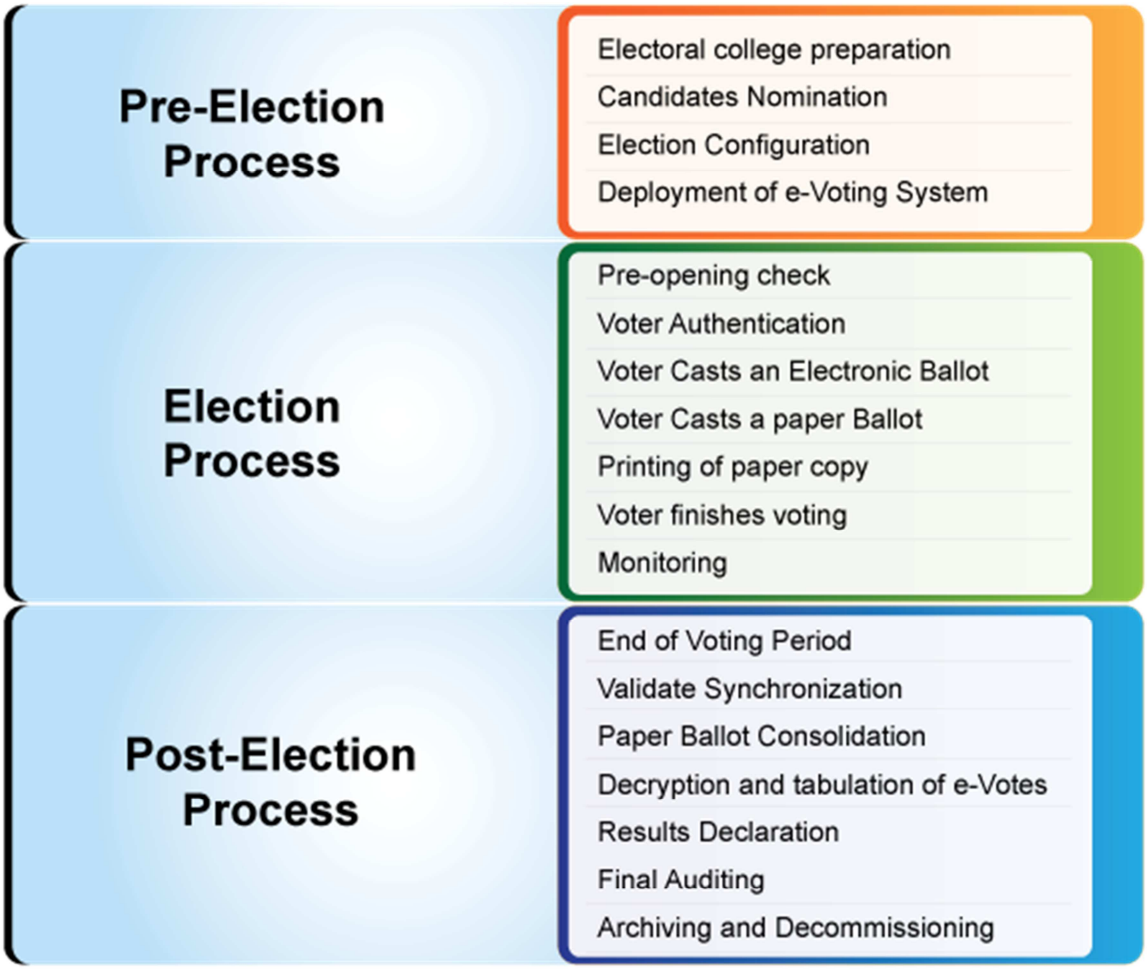


Figure 9: e-voting business process categories

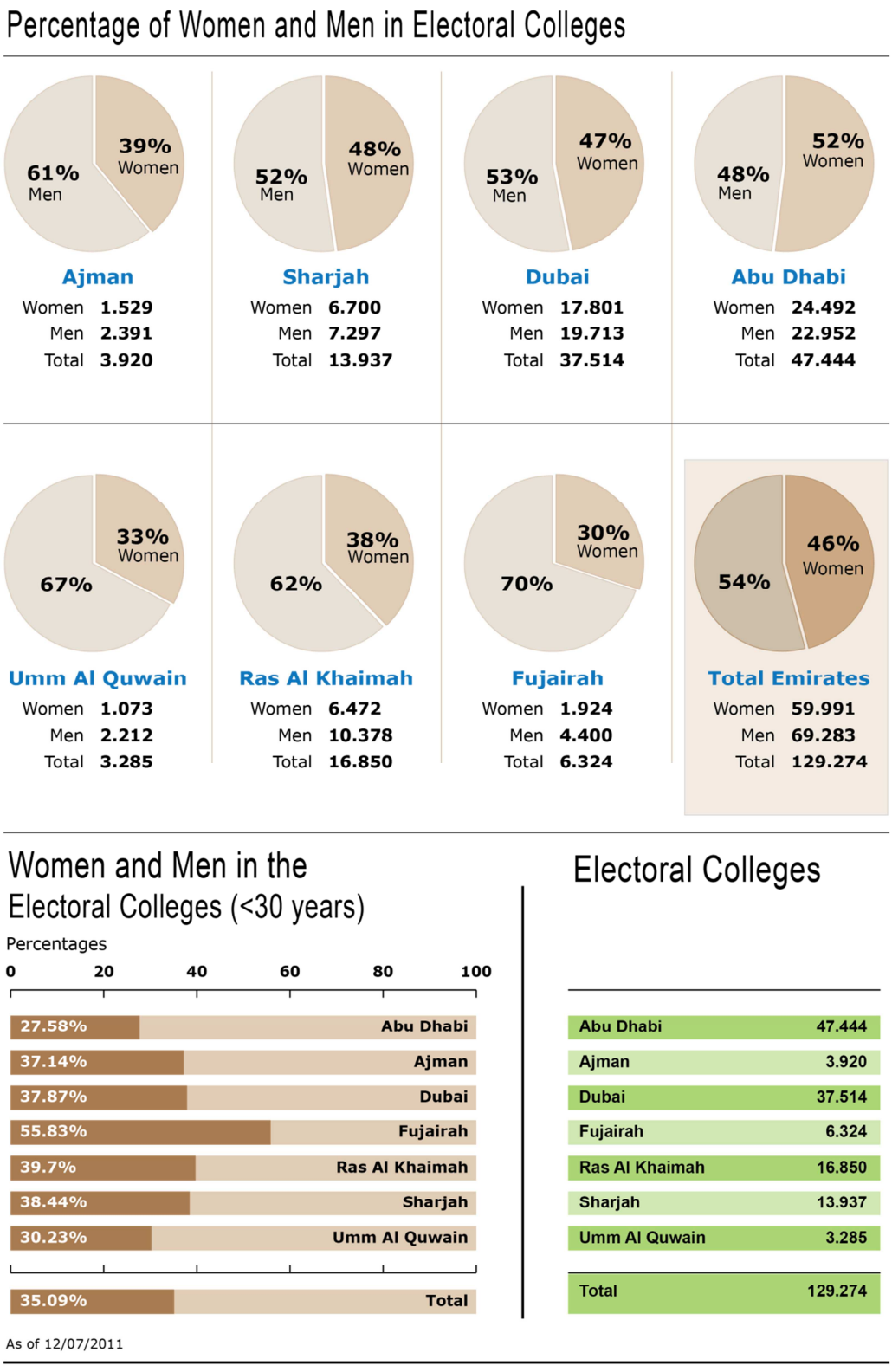


Figure10: FNC electoral college composition and demographics

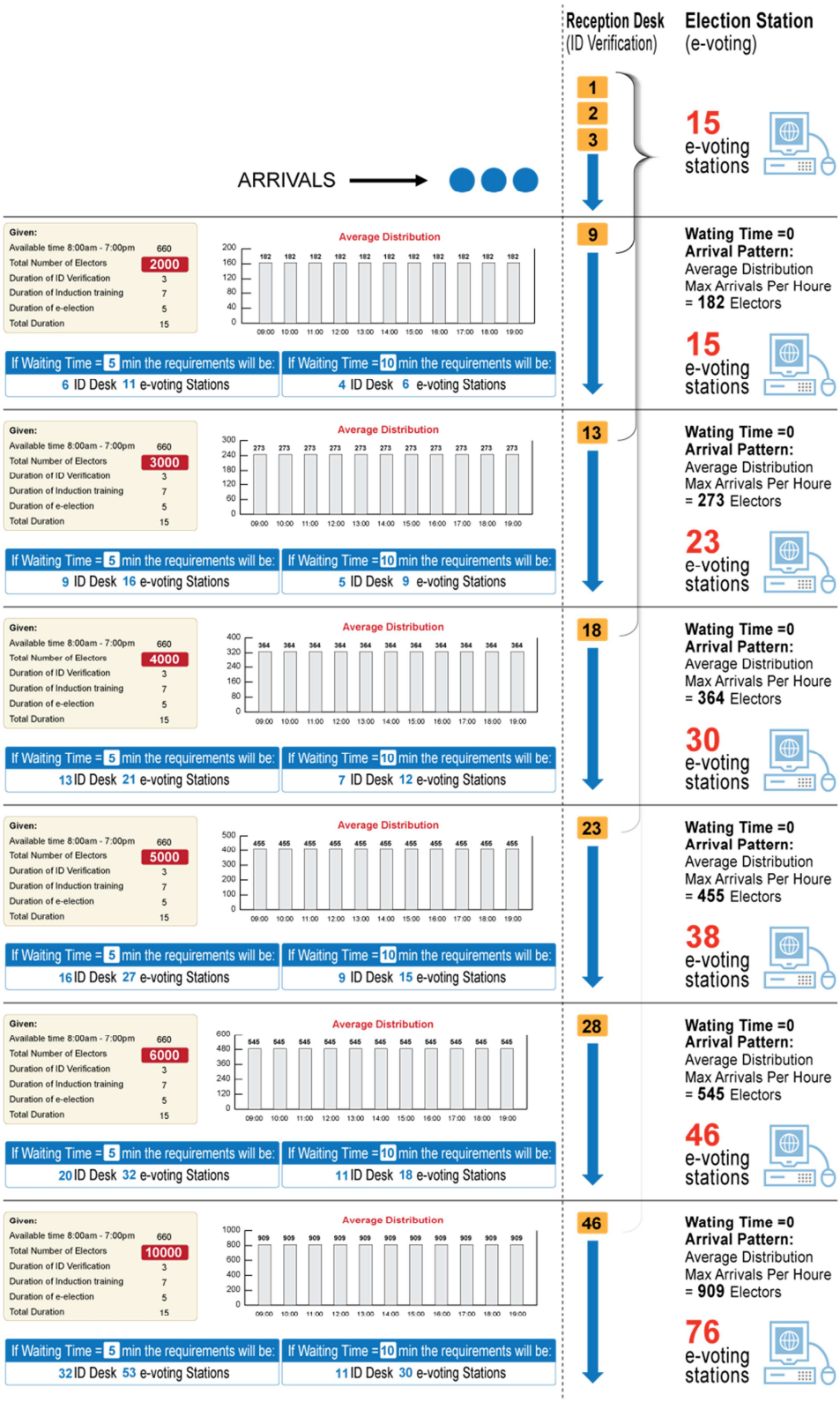


Figure 11: Calculation Scenarios

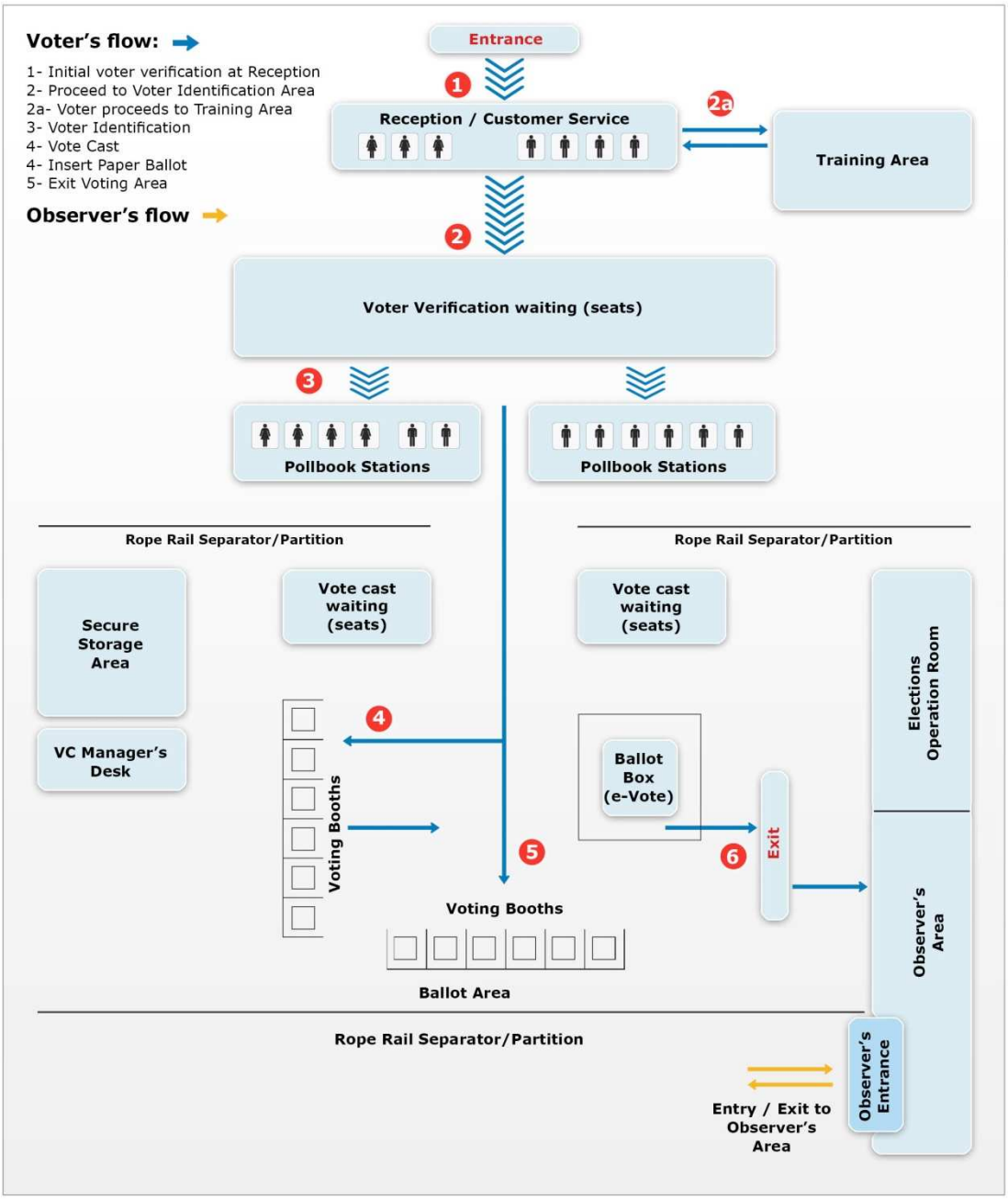


Figure 12: Voting centre layout

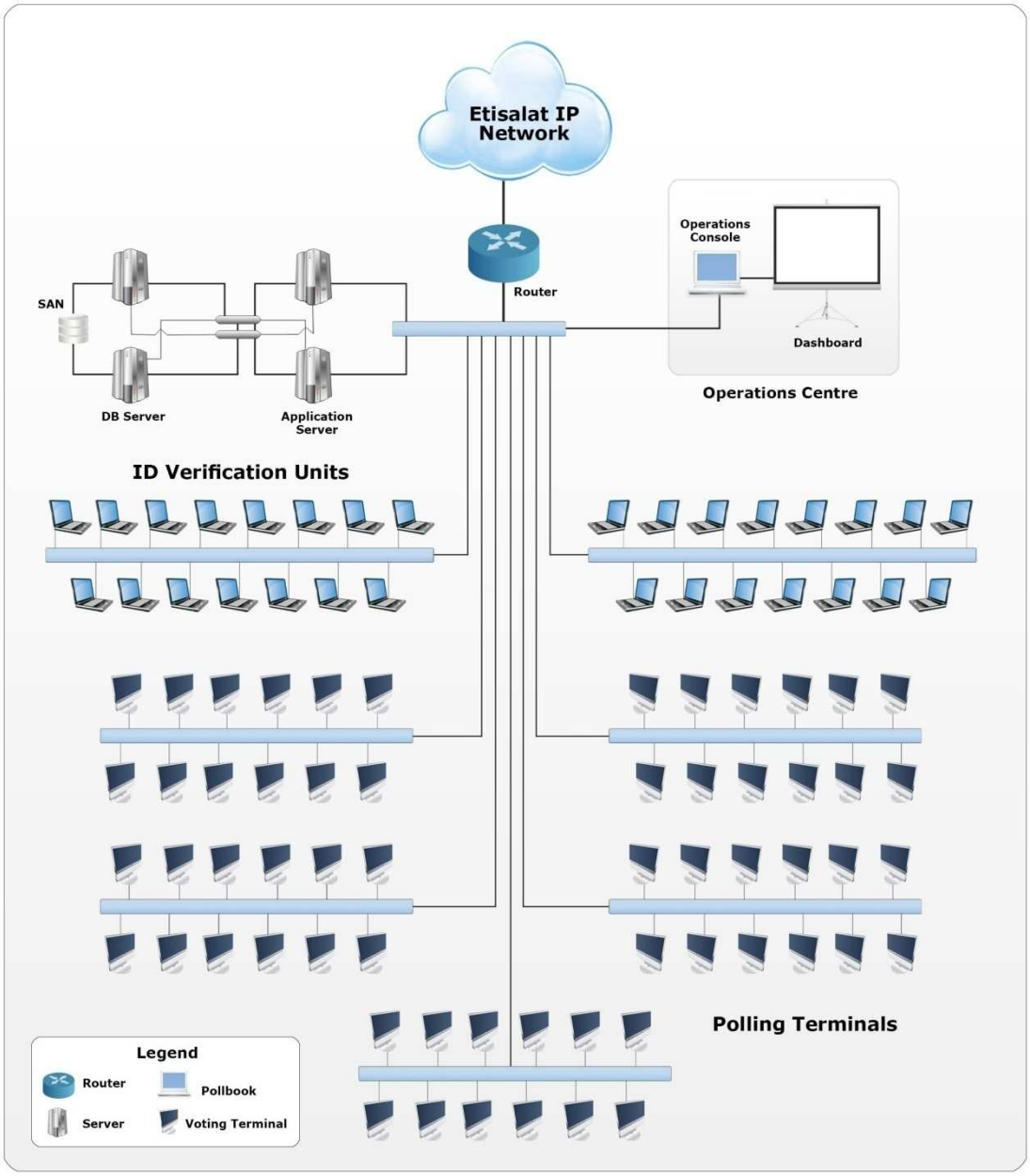


Figure 13: Voting site network design

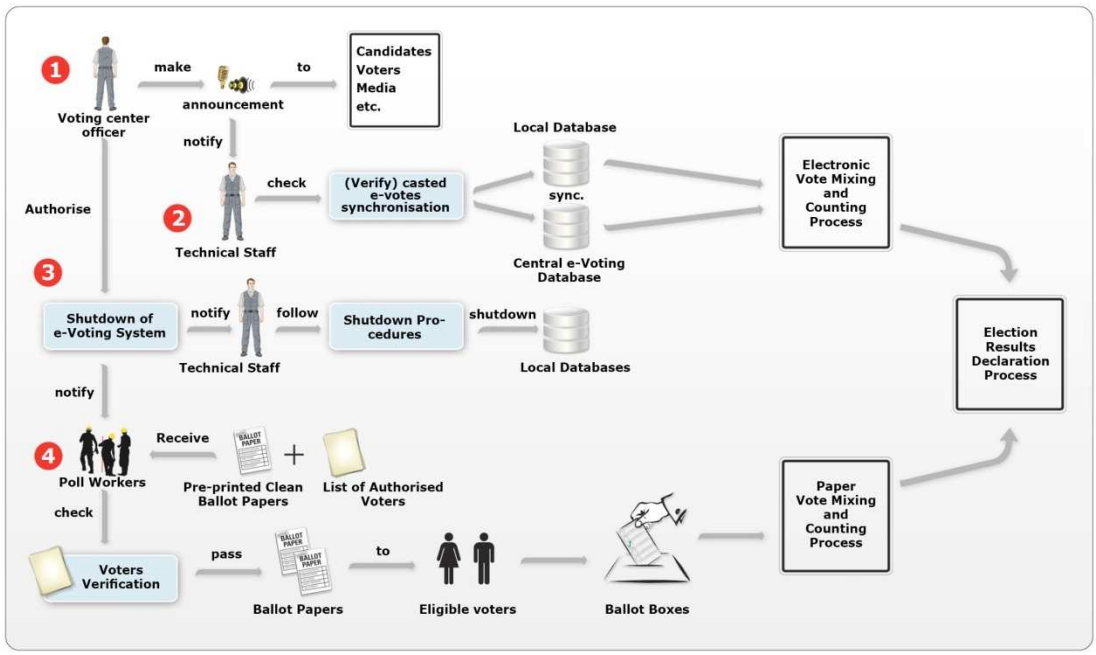


Figure 14: Procedures of switching to paper voting

Figure 15: Election day snapshot

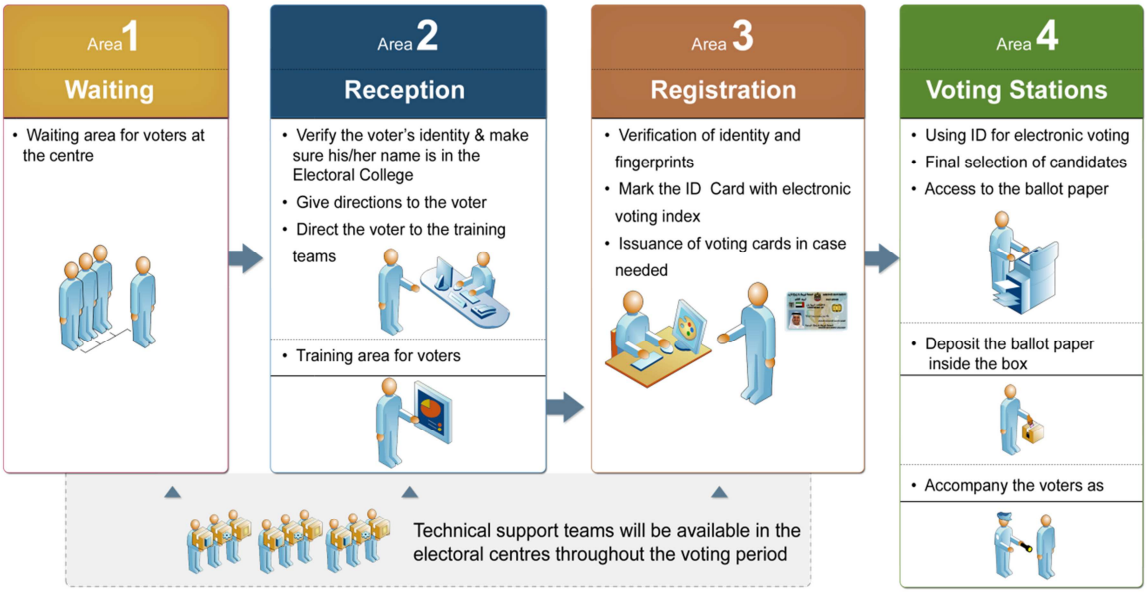


Figure 16: Voting procedures during election day

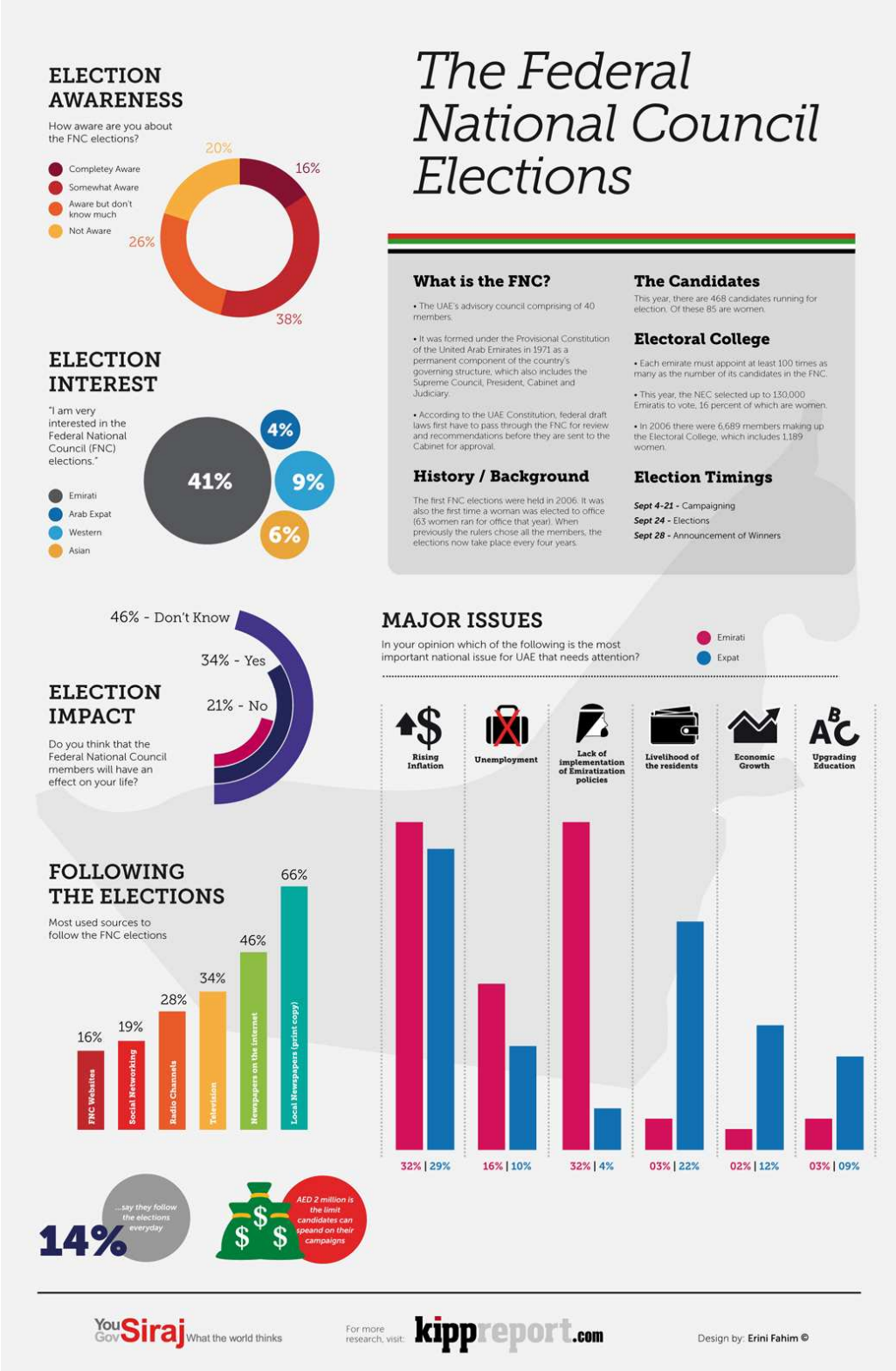


Figure 17: Kippreport survey results

Table 1: Types of e-voting systems

Voting system	Desc
Paper-based electronic voting system	Also referred to as "document ballot voting system", first emerged as a system where votes are casted and counted by hand, using paper ballots. With the advent of electronic tabulation came systems where paper cards or sheets could be marked by hand, but counted electronically. These systems included punched card voting, marksense and later digital pen voting systems. Most recently, these systems can include an Electronic Ballot Printers (EBPs), that allow voters to make their selections using an electronic input device, usually a touch screen system similar to a DRE machine, that produce a machine-readable paper or electronic token containing the voter's choice. This token is fed into a separate ballot scanner which does the automatic vote count..
Direct-recording electronic (DRE) voting system	A direct-recording electronic (DRE) voting machine records votes by means of a ballot display provided with mechanical or electro-optical components that can be activated by the voter (typically buttons or a touchscreen); that processes data with computer software; and that records voting data and ballot images in memory components. After the election, it produces a tabulation of the voting data stored in a removable memory component and as printed copy. The system may also provide a means for transmitting individual ballots or vote totals to a central location for consolidating and reporting results from precincts at the central location. These systems use a precinct count method that tabulates ballots at the polling place. They typically tabulate ballots as they are cast and print the results after the close of polling.
Public network DRE voting system (Internet voting systems	With internet voting systems, votes are transferred via the Internet to a central counting server. Votes can be casted either from public computers or from voting kiosks in polling stations or more commonly from any Internet-connected computer accessible to a voter.
OMR Systems	Optical and digital scanning systems which are based on scanners that can recognize the voters' choice on special machine-readable ballot papers. OMR systems can be either central count systems (where ballot papers are scanned and counted in special counting centres) or precinct count optical scanning (PCOS) systems (where scanning and counting happens in the polling station, directly as voters feed their ballot paper into the voting machine). These are normally used to improve the accuracy of the counting process and reduce potential manual counting errors. However, the quality of the count depends on the correct marking of the ballot paper and the quality of the ink used by the voter.
Polling stations	At a polling station, use of one medium to record the vote, which is then registered in a ballot box on another device. This system differs substantially from a DRE in that nothing is stored in the DRE and it is impossible for a voter to manipulate the memory containing the vote.

Table 2: Strengths and weaknesses of e-voting systems[5] Source: IDEA (2011)

Electoral issues. compared to paper voting	Internet voting	DRE with out VVPAT	DRE with VVPAT	PCOS	Electronic ballot printers
Faster count and tabulation	Strength	Strength	Strength	Strength	Strength
More accurate results	Strength	Strength	Strength	Strength	Strength
Management of complicated electoral systems	Strength	Strength	Strength	Strength	Strength
Improved presentation of complicated ballot papers	Mixed	Mixed	Mixed	Weakness	Mixed
Increased convenience for voters	Strength	Mixed	Mixed	Weakness	Mixed
Increased participation and turnout	Strength	Neutral	Neutral	Neutral	Neutral
Addressing needs of a mobile society	Strength	Mixed	Mixed	Neutral	Mixed
Cost savings	Mixed	Weakness	Weakness	Weakness	Weakness
Prevention of fraud in polling station	Neutral	Strength	Strength	Strength	Strength
Greater accessibility	Mixed	Mixed	Mixed	Weakness	Mixed
Multi-language support	Strength	Strength	Strength	Weakness	Strength
Avoidance of spoilt ballot papers	Strength	Strength	Strength	Strength	Strength
Flexibility for changes handling of deadlines	Strength	Strength	Strength	Weakness	Strength
Prevention of family voting	Strength	Neutral	Neutral	Neutral	Neutral
Lack of transparency	Weakness	Weakness	Mixed	Mixed	Mixed
Only experts can fully understand the voting technology	Weakness	Weakness	Mixed	Mixed	Mixed
Secrecy of the vote	Weakness	Mixed	Mixed	Mixed	Mixed
Risk of manipulation by outsiders	Weakness	Mixed	Mixed	Mixed	Mixed
Risk of manipulation by insiders	Weakness	Weakness	Weakness	Weakness	Weakness
costs of introduction and maintenance	Strength	Weakness	Weakness	Weakness	Weakness
Intrastructure / environmental requirements	Mixed	Weakness	Weakness	Weakness	Weakness
lack of e-voting standards	Weakness	Weakness	Weakness	Weakness	Weakness
Meaningful recount	Weakness	Weakness	Strength	Strength	Strength
Vendor - dependence	Weakness	Weakness	Weakness	Weakness	Weakness
Increased IT security requirements	Weakness	Weakness	Weakness	Weakness	Weakness

[5] Note: Details in the matrix would vary depending on specifics of context and systems. Cases where these details are very important are classified as 'mixed'; cases where e-voting has little or no impact are classified as 'neutral'. VVPAT: Voter-verified paper audit trail (VVPAT). PCOS: Precinct count optical scans.

Table 3: Research around e-voting systems

Researcher(s)	Contribution
Neumann (1993)	Recommended a list of generic voting criteria to enhance the security of the overall voting systems and resistance to failure. These include confidentiality, integrity, availability, reliability, and assurance for the involved computer systems. He also concluded that, **operationally, no commercial system is likely to ever meet all requirements, and that developing a suitable custom system would be extremely difficult and prohibitively expensive.**
Mercuri (1993; 2002)	Her philosophy is very similar to Neumann's . She invented her own method for electronic voting; also referred to as Mercuri method. Her method is similar to the Caltech/MIT proposal where the voting machine in her **method is designed to produce human-readable hardcopy paper results, which can be verified by the voter before the vote is casted**, and manually recounted later if necessary.
Chaum (2004)	Presented a worthy to note system design that provides voter verifiability, i.e., to provide voters with the capability to verify that their vote is accurately included in the tally - even if all election computers and records were compromised. **Such trust would provide a high degree of transparency** that allows close auditing of the vote capture and counting process if needed. Chaum's proposed system design preserves ballot secrecy, while improving access, robustness, and adjunction, all at lower cost.
Shamos (1993)	Provided a sharp counterpoint to Neumann and Mercuri's views, but was less impressed with paper ballots than are Neumann and Mercuri. He recommended DRE machines with decentralization design to make fraud difficult to commit and easy to detect. He contribution also involved the development of "Six Commandments "summary of requirements for a voting system. The list of requirements can be used to critique voting systems and as basis for public inspection.
Kosmopoulos (2004); Rivest (2004)	Pointed out issues related to the development of **secure platforms** and issues related to the **simplification and usability of voting machines, development of audit-trails, support for disabled voters,** security problems of absentee ballots, etc.
Clausen et al. (2000)	Presented a **secure electronic polling system** which does not rely on persistent network connections between polling places and the vote-tallying server. They build the system on a disconnected (or, more accurately, an intermittently connected) environment, which **works well in the absence of network connectivity.**
Volkamer (2009)	Stressed on the need to provide a **trustworthy base for secure electronic voting,** and how to **prevent accidental or malicious abuse** of electronic voting in elections. Others refer to the opaque nature of the technologies involved, which few understand, and that it is crucial that electronic voting systems provide a **voter-verifiable audit trail,** which will act as a permanent record of each vote that can be checked for accuracy by the voter before the vote is submitted, which will make it difficult or impossible to alter after it has been checked (Kosmopoulos, 2004).
Klein (1995)	Presented a remote voting system design to higher the levels of **privacy, universal verifiability, convenience and untraceability,** but at the expense of receipt-freeness. The suggested design applies the technique of blinded signature to a voter's ballot so that it is impossible for anyone to trace the ballot back to the voter.

Table 4: Voting Systems Requirements

Requirement	Description
Privacy	To ensure the secrecy of the ballots.
Universal Verifiability	To ensure that all valid votes have been included in the final tally.
Robustness	The system can tolerate a certain number of faulty participants.
Receipt-freeness	The voters cannot provide a "receipt" that shows what they voted.
Fairness	No partial tally is revealed before the end of the elections.
Dispute-freeness	The fact that the participants follow the protocol at any phase can be publicly verified by any casual third party.
Self-tallying	The post-ballot-phase can be performed by any interested third party.
Ballot Secrecy	To ensure secrecy of what takes place. The only thing revealed about the voters' choice is the final result.
Authentication	Ensure that individuals cannot be impersonated.
Accuracy	Ability to ensure that each individual's vote is recorded and counted.
Timelines	To record information and to have the results available quickly.
Accessibility	To have a system that is accessible to all and easy to use.
Security	To guard against manipulation and interference.

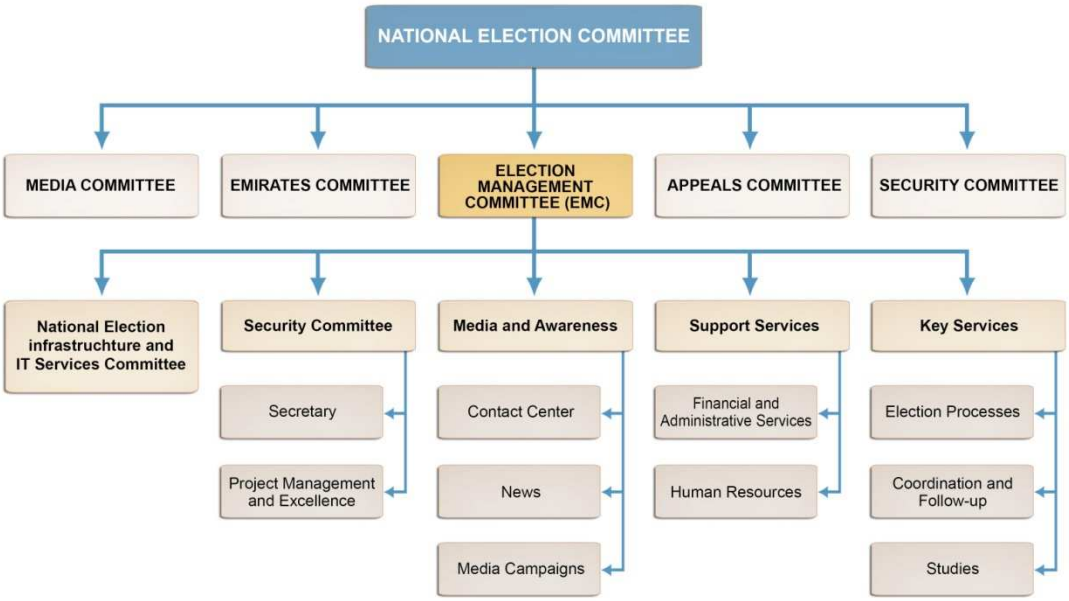
Table 5: e-voting design principles

Objective	Desc.
Voter Authenticity	the voting platform shall ensure only eligible voters are allowed to vote.
Voter Anonymity	The voter privacy regarding the selected voting options shall be protected at all levels. Nobody – including the system administrators and election authorities– shall be able to associate a voter's ID with his selected voting options.
Election Integrity	The election system shall ensure only one ballot is cast per eligible voter, and ballots are processed and counted as defined.
Service Availability	The voting platform shall be available during the prescribed election time limits.
Open Auditing	It shall be possible to demonstrate the accuracy, integrity, and fairness of the election process.
Service Protection	All the components from the voting services shall be resistant to system failures, denial of service and security attacks.

Table 6: Pilot test constituents

Objective	Description
Environment	A mock election instance was setup in the local servers at the voting centre.
Test Material	1. File dump was prepared with electoral roll and the candidates 2. A mock election was defined and configured for a. Institution, Election Event and Election identification b. Dates, start and end time c. Electoral rules (replica of actual election rules) Users in each user role were identified and teams constituted to complete end to end voting process.
Equipment	Complete voting centre setup comprising of all equipment (servers, network, switches, voting terminals, voter identification terminals, ID card readers, biometric readers etc) required at the voting centre on the election day were put in place. Dry run participants used both the national ID cards and the contingent white smart cards to cast the votes.
Resources	Emirates identity authority mobilized nearly 600 of its staff to participate in the dry run in addition to the people deployed from Takatuf (an organization providing volunteers). A formal mock Electoral Board was constituted and the pilot election was opened for voting.
Communication	A key element in the pilot planning was communication. A detailed communication plan was worked out and resources were reached out to make the dry run a success.

Annex-1: Functions and Responsibilities of the National Election Commission and its sub-committees



1. National Election Commission (NEC)

The National Election Commission (NEC) was formed in February 2011 by a presidential decree consisting of government officials and public figures. The National Election Committee (NEC) was empowered to oversee the whole election process, including:

- Setting out the overall Election Framework
- Supervising the elections
- Supporting efforts to raise electoral awareness
- Writing down elections guidelines
- Locating Polling Centres in each Emirate
- Approving regulatory measures for establishing the electoral legal framework
- Issuing and seeking approval for the governing rules for the lists of Electoral Panels Members
- Setting the date of elections

2. Election Management Committee

- Directing, supervising, and monitoring its staff as per applicable regulations and NEC decisions.
- Coordinating with relevant bodies, and coordinating subcommittees activities in these bodies, to ensure full implementation of prescribed duties and functions.
- Identifying manpower and financial needs required for implementing assigned tasks and reporting them to NEC.
- Recommending necessary decisions and regulations for the functions of Election Management Committee (EMC), and its subcommittees; and reporting them to NEC for approval, and monitoring their implementation.
- Monitoring the implementation of NEC electoral decisions and guidelines directed to subcommittees concerning the preparation for elections, and reporting the same to NEC in a timely manner.
- Preparing elections budgets.
- Taking all necessary actions to ensure safety of elections.
- Assessing appeals for later submittal to NEC.
- Submitting statements of votes to NEC, before announcing final results.
- Any other functions assigned by NEC.
- The Committee may take all necessary steps for the implementation of its assigned tasks. It may also procure the services of experienced professionals, as appropriate.

2.1 Project Management and Excellence Committee

- Suggesting strategic and operational plans; and setting out and prioritizing policies, and how to measure them.
- Preparing and developing these plans, along with work programs, in coordination with other relevant organizational units in the Committee.

- Designing performance indicators, and submitting performance reports to all these units in the Committee and concern parties.
- Monitoring strategic plans, evaluating performance and enhancing services at EMC. The Office shall also provide appropriate procedures, evidences, and systematic documentation for all operations, based on excellence requirements.
- Managing projects based on established methodologies.
- Ensuring excellence criteria are met in all measures taken.
- Handling Chairman of the Committee's reports and correspondence, whilst making all necessary arrangements and follow-ups for his meetings with relevant bodies.
- Measuring all concern parties results and conducting excellence-compliant questionnaires

2.2 Infrastructure and IT Services Committee

- Implementing EMC-approved policies, strategies, standards, procedures, and regulations
- Providing highly effective IT services to cope with elections needs.
- Identifying IT programs and systems requirements to enhance networking connections as required for Election Management Committee, whilst setting the IT work plan and needs.
- Designing and developing computer systems to be used for elections, and ensuring they meet preset standards.
- Setting IT budget.
- Documenting the system throughout deployment and operation phases.
- Supervising the upgrading of IT networks required for making well-developed systems.
- Checking the specifications of networks and connection lines currently in operation
- Preparing and presenting back-up plans in cases of emergencies.
- Training systems users; informing them of their advantages and methods of operation.
- Technically supervising the website, in coordination with the Media and Communications and Electoral Processes Unit.
- Laying down different scenarios for e-voting, in terms of connection and IT requirements.
- Ensuring the readiness, safety, and security of IT systems.
- Providing all IT needs for media centres and Polling Centres.
- Any other functions assigned by EMC.

2.3 Key Services

2.3.1 Election Processes

- Setting and implementing relevant policies, strategies, standards, and procedures for highly efficient electoral service provision
- Preparing, saving, and classifying Electoral Panel members' records and databases
- Informing Panel members of their electoral responsibilities
- Registering Electoral Panel members
- Updating Panel members databases
- Organizing and registering candidates
- Identifying the appropriate method for announcing the Names of the Electoral Panel Members (Newspapers, phone calls, or SMS)
- Coordinating with the 7 Emirates Rulers' courts to acquire the names of the Electoral Panel Members
- Providing an appropriate form which includes all required data of the Panel Member. This form must meet and befit electoral needs and requirements and facilitate research and studies
- Launching and updating website pages displaying the names of the Electoral Panel Members in coordination with the Media and Communication Unit and the IT Committee
- Furnishing the Contact Centre with the Electoral Panel Members' names

2.3.2 Coordination and Follow-up

- Streamlining communications and follow-up for different Emirates committees.
- Monitoring how far Committees' decisions are put into action.
- Assessing and handling complaints and feedbacks, except for appeals.
- Working closely with election partners; by showing good understanding and response to their needs.
- Providing all what is necessary to enhance coordination between the Emirates committees and the Election Committee, whilst enacting relevant procedures by arranging Committees' agendas, documenting their individual minutes, monitoring the implementation of recommendations, and fully

coordinating with relevant bodies concerning the functions of the Emirates Committees Coordinator, and any other relevant coordinating functions.

2.3.3. Studies

- Setting goals and plans for research and studies according to Committee requirements, whilst supervising the implementation of each.
- Providing research, advisory, and consultation services concerning electoral affairs.
- Conducting research, studies, questionnaires, and evaluation forms that aim at measuring public opinion trends concerning EMC activities and related issues.
- Preparing reports, briefs, whitepapers, and working papers for the Committee to submit to other entities.
- Setting and implementing information service plans based on the Committee's needs
- Preparing the final NEC Report.
- Collecting data and statistics.
- Providing the Committee with the studies and research required.
- Reporting candidates' expenditures in election campaigns.
- Managing legal affairs and auditing procedures.

2.4 Support Services

- Setting and implementing policies, strategies, standards, and procedures for providing highly effective human resources services
- Planning human resource requirements and preparing necessary budgets
- Setting job plans and descriptions for human resources required for elections
- Attracting and selecting competent staff (permanent/temporary/reserve)
- Registering staff and issuing ID cards
- Training (staff in elections/ contact centres)
- Distributing staff and managing their affairs
- Personnel affairs management during elections
- Developing an appropriate method for calculating compensation of staff participating in administering elections

2.4.1 Financial and Administrative Services

- Setting and implementing policies, strategies, standards, and procedures for providing highly effective administrative and financial services
- Preparing budgets for Election Management Committee , and monitoring budget execution
- Performing purchase procedures, settling due amounts, and issuing checks
- Passing accounting entries in different original journals
- Preparing budget allocated for the committee, setting budget for media campaign/ technological needs/ office needs/ logistic requirements/ Polling Centres/ hospitality/ reception/ transportation/ accommodation, etc
- Establishing compensation system for committees members/staff organizing elections/subcommittees
- Setting and managing petty loans for officials at Polling Centres
- Collecting fees (for registration/appeals)
- Conducting EMC-related public relations (PR) activities
- Identifying the type of forms, applications, and reports specifically required and used in elections
- Supplying Polling Centres with all required equipments
- Providing accommodation and transportation for invited media representatives, between the hotels and the Polling Centres
- Providing logistic needs and services for Polling Centres and media centres
- Arranging official communications and correspondence with other regulatory bodies and units based on applicable powers
- Managing archiving processes

2.4.2 Human Resources

- Setting and implementing policies, strategies, standards, and procedures for providing highly effective human resources services
- Planning human resource requirements and preparing necessary budgets
- Setting job plans and descriptions for human resources required for elections
- Attracting and selecting competent staff (permanent/temporary/reserve)

- Registering staff and issuing ID cards
- Training (staff in elections/ contact centres)
- Distributing staff and managing their affairs
- Personnel affairs management during elections
- Developing an appropriate method for calculating compensation of staff participating in administering elections

2.5 Media Awareness

- Implementing the communication strategy as per the "Guide for Media Handling of the Elections"
- Implementing the draft plan prepared for the media and advertising campaigns
- Carrying out different media-related activities and developing effective communication tools with relevant parties
- Holding regular meetings with Editors-in-Chief and journalists covering the elections to keep them updated
- Supervising media centres, coordinating with mass media, and providing coverage materials, and bilingual media coordinators (fluent in Arabic and English)
- Training official spokesmen on how to deal with the media and relevant messages
- Enacting regulations for communicating with media officials for elections officers to abide by
- Monitoring media coverage of NEC, FNC Elections and political participation in UAE, whether in local or global mass media
- Distributing official elections results over media entities
- Allocating special areas and seats for media representatives at every Polling Centres
- Informing Panel members of their electoral responsibilities, in coordination with the Electoral Processes Unit
- Holding informative sessions about political participation, along with discussion panels and groups that cover the elections issue

2.5.1 Contact Centre

- Implementing the communication strategy as per the "Guide for Media Handling of the Elections"
- Implementing the draft plan prepared for the media and advertising campaigns
- Carrying out different media-related activities and developing effective communication tools with relevant parties
- Holding regular meetings with Editors-in-Chief and journalists covering the elections to keep them updated
- Supervising media centres, coordinating with mass media, and providing coverage materials, and bilingual media coordinators (fluent in Arabic and English)
- Training official spokesmen on how to deal with the media and relevant messages
- Enacting regulations for communicating with media officials for elections officers to abide by
- Monitoring media coverage of NEC, FNC Elections and political participation in UAE, whether in local or global mass media
- Distributing official elections results over media entities
- Allocating special areas and seats for media representatives at every Polling Centres
- Informing Panel members of their electoral responsibilities, in coordination with the Electoral Processes Unit
- Holding informative sessions about political participation, along with discussion panels and groups that cover the elections issue

2.5.2 News

- Implementing the communication strategy as per the "Guide for Media Handling of the Elections"
- Implementing the draft plan prepared for the media and advertising campaigns
- Carrying out different media-related activities and developing effective communication tools with relevant parties
- Holding regular meetings with Editors-in-Chief and journalists covering the elections to keep them updated
- Supervising media centres, coordinating with mass media, and providing coverage materials, and bilingual media coordinators (fluent in Arabic and English)
- Training official spokesmen on how to deal with the media and relevant messages
- Enacting regulations for communicating with media officials for elections officers to abide by

- Monitoring media coverage of NEC, FNC Elections and political participation in UAE, whether in local or global mass media
- Distributing official elections results over media entities
- Allocating special areas and seats for media representatives at every Polling Centres
- Informing Panel members of their electoral responsibilities, in coordination with the Electoral Processes Unit
- Holding informative sessions about political participation, along with discussion panels and groups that cover the elections issue

2.5.3 Media Campaigns

- Implementing the communication strategy as per the "Guide for Media Handling of the Elections"
- Implementing the draft plan prepared for the media and advertising campaigns
- Carrying out different media-related activities and developing effective communication tools with relevant parties
- Holding regular meetings with Editors-in-Chief and journalists covering the elections to keep them updated
- Supervising media centres, coordinating with mass media, and providing coverage materials, and bilingual media coordinators (fluent in Arabic and English)
- Training official spokesmen on how to deal with the media and relevant messages
- Enacting regulations for communicating with media officials for elections officers to abide by
- Monitoring media coverage of NEC, FNC Elections and political participation in UAE, whether in local or global mass media
- Distributing official elections results over media entities
- Allocating special areas and seats for media representatives at every Polling Centres
- Informing Panel members of their electoral responsibilities, in coordination with the Electoral Processes Unit
- Holding informative sessions about political participation, along with discussion panels and groups that cover the elections issue

3. Emirates Committee

- Coordinating with the EMC about technical and administrative electoral issues in the Emirate, and more specifically:
- Locating Committee office whilst maintaining communications with EMC
- Receiving the final list of the electoral panel and sending it to Committee members
- Receiving electoral forms from EMC and providing them in the Committee office
- Coordinating with the Emirate's police to provide for the sufficient number of police officers on election day, as per the election Security Committee guidelines
- Collaborating with the local Municipality, jointly with EMC
- Recommending Polling Centres location(s) in the Emirate, in coordination with EMC
- Advising candidates of places for holding election rallies
- Assessing the Emirate nominations against preset requirements before submission to EMC
- Assessing appeals for providing all information required before submission to EMC
- Monitoring compliance with election controls and measures and reporting any violations to EMC
- Performing any other functions within the authority of the Committee

4. Appeals Committee

- Drafting and implementing the appeals administration process
- Reviewing and handling appeals concerning voters' registration and the electoral roll
- Reviewing and handling appeals concerning lists of candidates and their registration
- Reviewing and handling appeals against voting results
- Reviewing and handling appeals of any administrative violations during elections
- Any other function within the authority of the Committee

5. Media Committee

- Raising public awareness of elections and encouraging their participation
- Coordinating with different media channels to raise public awareness of the Federal National Council elections

- Setting and implementing consolidated media policies, standards, strategies, and procedures (before, during, and after elections)
- Developing and implementing media programs and plans required for the elections
- Developing a guide on how the Media (whether visual, broadcast, or print media) covers and handles the elections
- Coordinating the use of official mass media in presenting candidates' programs to ensure equal-opportunity exposure
- Organizing press conferences and maintaining media centres before, during, and after elections
- Collaborating with partner professional media firms
- Performing any other functions within the authority of the Committee

6. Security Committee

- Drafting and implementing security plan for elections
- Developing security rules and criteria for Polling Centres to follow
- Enacting consistent security measures for implementation at these Polling Centres
- Identifying methods of dealing with election-day issues and problems
- Coordinating the provision and implementation of safety and security procedures and standards with every possible means
- Any other function within the authority of the Committee

Annex-2:

A2-1 Requirements Definition Workshop

The Business Process requirements workshops spanned over four sessions and covered the following:

Session 1	
Title:	**Business Processes**
Objectives:	Agree on business processes. Demonstrate process mapping to existing e-Voting functionality, in order to identify gaps
Attendees:	All key business representatives; NEC's Legal advisor on Electoral Matters
Topics:	1. Introduction - Objective of Workshop and next steps 2. Processes • Before Election Day • During Election Day • After Election Day 3. As-is solution demo mapping to these processes 4. Regulatory and legal implications

Session 2	
Title:	**Solution Functionality and User Interfaces**
Objectives:	Review and agree on proposed functionality for key solution components and agree on content/functionality of user interfaces
Attendees:	Business Owners and End user representatives
Topics:	1. Details of functionality of each application 2. Basic wireframes to capture requirements related to screen content • Pollbook • Dashboard • Web Reporting • Voting Screens and Back office

Session 3	
Title:	**Location, Roles and Responsibilities**
Objectives:	Agree on high level requirements for different types of locations, understanding theconstraints and roles required at each location. Identify exception handling and legal implications.
Attendees:	EIDA/NEC Technical Team; NEC Procurement; Election Organizers; NEC Legal Advisor on Electoral Matters
Topics:	1. Details of requirements and staff roles at each of the following locations • Data Centre • Election Operations Centre • Warehouse/testing site • Voting centers 2. Non-functional requirements 3.Exceptions handling processes 4. Regulatory and legal implications

Session 4	
Title:	**Information Exchange**
Objectives:	Discuss and agree on information exchange requirements
Attendees:	EIDA/NEC Technical Team; EIDA/NEC staff who know about Voter and Candidate information and its format
Topics:	1. Voter validation/authentication • Integration with UAE ID Card 2. Information Exchange • Import Information: Voters list, Candidate names and pictures • Export Information: what information is to be exported from the system after election 3. Review BOM with details of equipment

These e-voting processes across the three stages are described here in terms of:

1. Business Process diagrams which illustrate tasks, both manual and automated, and the roles involved in the execution of end-to-end electronic voting process, using the voting software.
2. Task description table that describe the various steps in the automated process.

   Each section includes a business process diagram supported by a table listing process steps. Input, output and pre-requisites for each key process are also described with the process steps description.

Figure A2-1: Key to symbols used in business process illustrations

A2-2 E-Voting Process Diagram

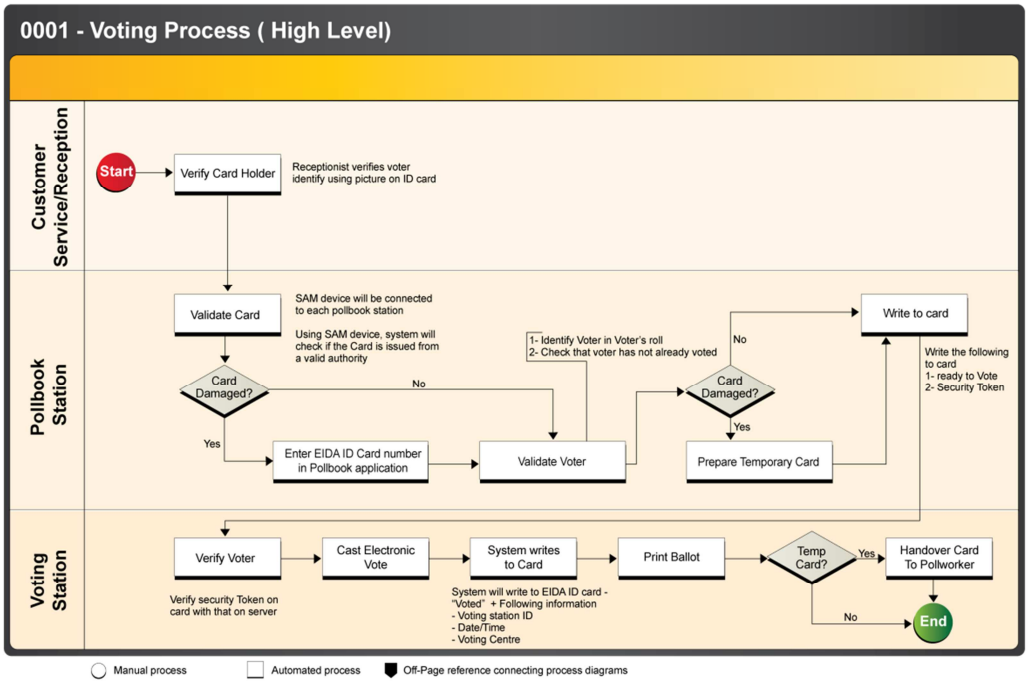


Figure A2-2: High level voting process

A2-3 Pre- Election Processes

After the system preparation and sealing steps have been completed, Election shall be configured following the Election Configuration process.

Next we describe the steps required to accomplish this task.

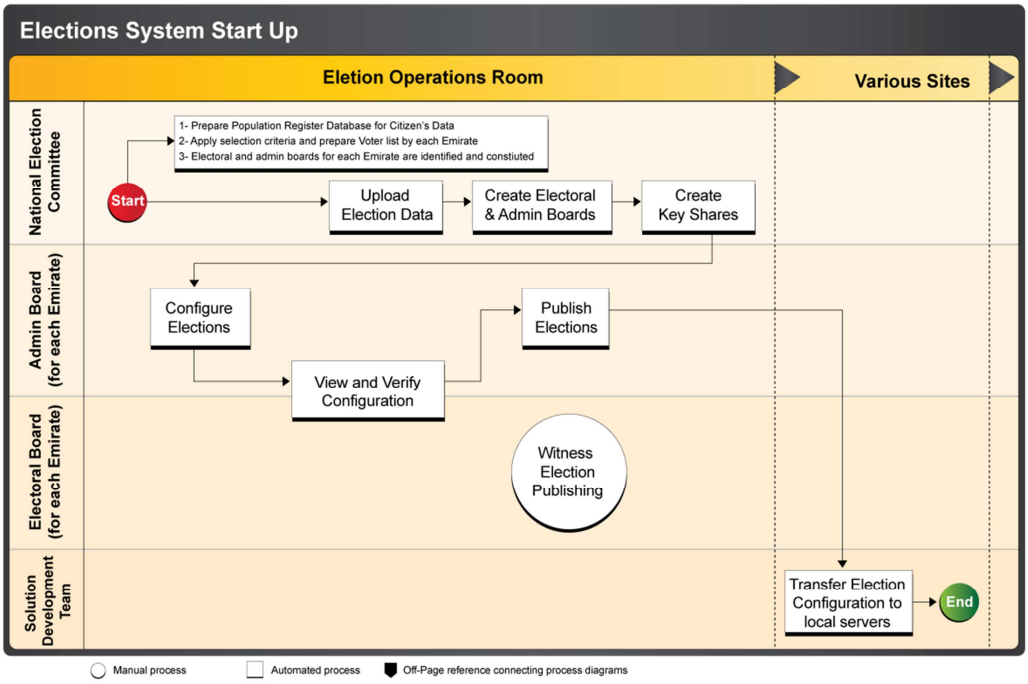


Figure A2-3: Elections System Start Procedures

Table A2-1: Pre-election technical process steps

Process Steps			
Steps	**Where**	**Who**	**Comments**
SOFTWARE PREPARATION			
1. Emirates ID Provides Population Register Database to each Emirate for preparing the Electoral Roll and finalize the list of eligible voters.	All Seven Emirates	Local Authorities in each Emirate and the Ruler's Courts	
1. The required Certificate Authority (CA) for the election is created, and any related keys are also created.	EIDA PKI system	EIDA and Solution Provider	
1. The voting software is compiled and built in a trusted environment in a suitable place.	Test site	Solution Provider	
4. The built software is deployed: • In the data centre • In all the voting servers located in the test site • Voting terminals and ID Verification units	Several locations	Solution Provider and Election Authority	
SYSTEM SEALING			
5. The servers in the data centre are logically sealed. • Database is physically and logically secured	Several locations	EIDA	

A2-3.1 Configure Elections Process

Once the system is setup the Election Configuration process is executed for each Emirate, in the presence of the Electoral and Admin board of that Emirate.

Inputs: For each Emirate: Voters list, Candidates list, Voting rules, Election timings.

Outputs: Election configured and published

Pre-Requisites:

i) All information required to configure election is provided by National Election Committee in the desired format

ii) Electoral and Admin boards for each Emirate are formed.

iii) Staff for required roles are assigned and available

Table A2-2: Configuration of Elections Process

Process Steps			
Steps	**Where**	**Who**	**Comments**
ELECTION CONFIGURATION			
The election is configured • Election general data, according to reference manual. • The file(s) with candidates and pictures (associated to each Emirate) is uploaded in the voting system • The file with the electoral roll (list of voters associated to each Emirate)	Operations Centre	Business Owner Auditor	DEPENDENCY: NEC to provide required files and information to configure the election in the agreed formats and times.
Each **Electoral and Administration Boards** are created in the correspondent Operational Center server following a secret sharing scheme process: • The Administration Board is required to publish the election and to do some administration operations • The Electoral Board holds the key required to decrypt the cast ballots and to sign election results.	Operations Centre	Business Owner Electoral Board Admin Board	**DEPENDENCY:** Business Owner to determine size and threshold for both boards. • Both boards can be merged in one, but we strongly suggest to keep them separated to reduce the number of operations to be done by the potentially high profile persons that will compose the Electoral Board. • The Admin Board is usually composed by more technical persons that the Electoral Board trust to delegate such tasks.
The election is published, i.e. its configuration is generated and exported so it can be deployed in the other voting servers of each Emirate: • Any stakeholder can review the configured data (candidates, dates, etc.) • The admin board signs the exported data in the publishing process	Operations Centre	Business Owner Auditor Admin Board	• Deployment on each voting center server by Emirate
Each Electoral and Administration Boards are created in the correspondent Operational Center server following a secret sharing scheme process: • The Administration Board is required to publish the election and to do some administration operations • The Electoral Board holds the key required to decrypt the cast ballots and to sign election results.	Operations Centre	Business Owner Electoral Board Admin Board	**DEPENDENCY:** Business Owner to determine size and threshold for both boards. • Both boards can be merged in one, but we strongly suggest to keep them separated to reduce the number of operations to be done by the potentially high profile persons that will compose the Electoral Board. • The Admin Board is usually composed by more technical persons that the Electoral Board trust to delegate such tasks.

Table A2-2: Configuration of Elections Process (Cont.)

Process Steps

Steps	Where	Who	Comments
ELECTION CONFIGURATION			
The election is published, i.e. its configuration is generated and exported so it can be deployed in the other voting servers of each Emirate: • Any stakeholder can review the configured data (candidates, dates, etc.) • The admin board signs the exported data in the publishing process	Operations Centre	Business Owner Auditor Admin Board	• Deployment on each voting center server by Emirate
The configuration files generated on each Operational Centre Server are transferred to the data centre servers: • They are uploaded and deployed on each voting centre servers of the correspondent Emirate. • They are uploaded and deployed on each Instance of the solution of the correspondent Emirate in the DC	Test Site	Business Owner Auditor Admin Board	**Exceptions:** **Issue:** No connectivity to data centre. **Solution:** take the DVD manually to data centre and testing site
FINAL DEPLOYMENT TESTING			
Deployment is validated and each decentralized voting server is sent to its destination voting centre	Several sites	System Integrator	**Additional logical sealing** can be done on the directories containing election configuration files.
Final Deployment Testing is performed: • Connectivity from voting centres' voting terminals and pollbooks • Dashboard	Each voting centre Operations centre	System Integrator	

A2-4 Election Day Process

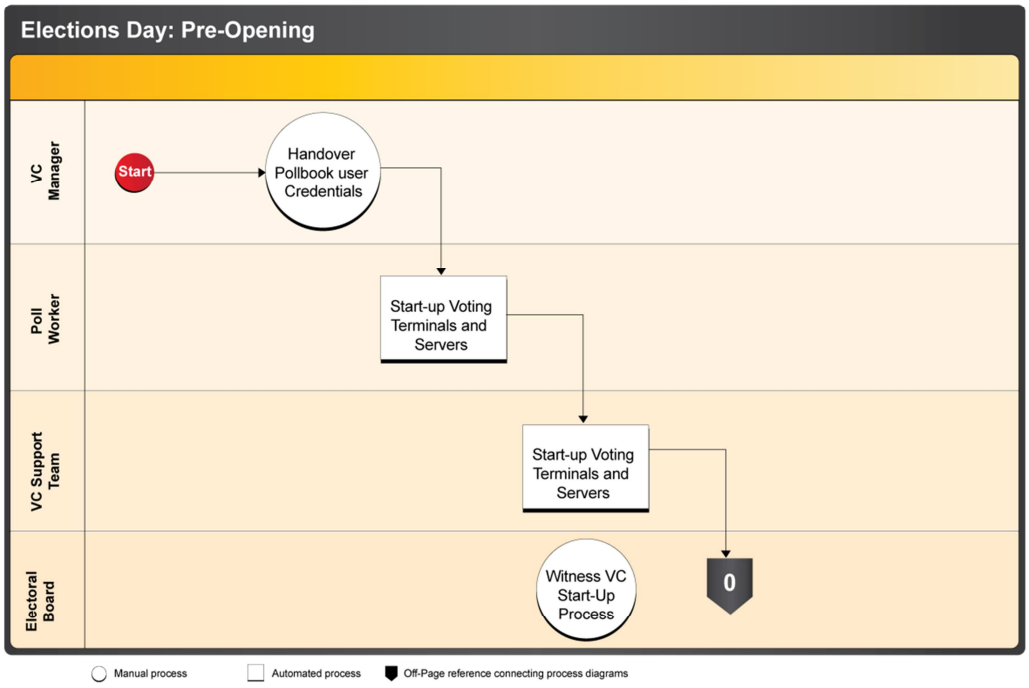


Figure A2-4: Business Process Diagram (Election Date)

Once the voting centre is opened for votes, the Voting process on the Election Day shall proceed in three stages.

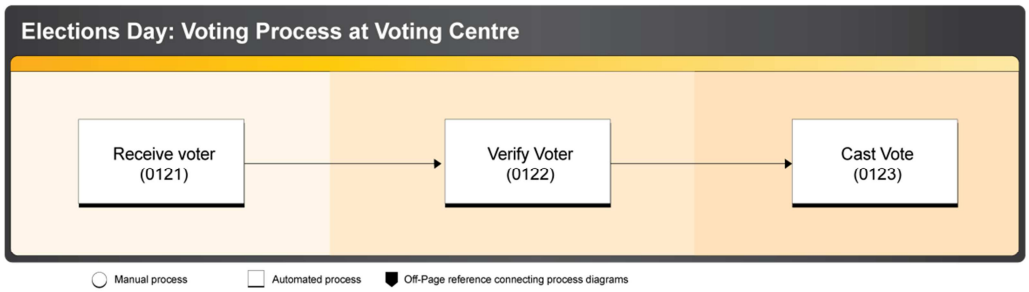


Figure A2-5: Voting process at election day

A detailed process diagram for each stage follows:

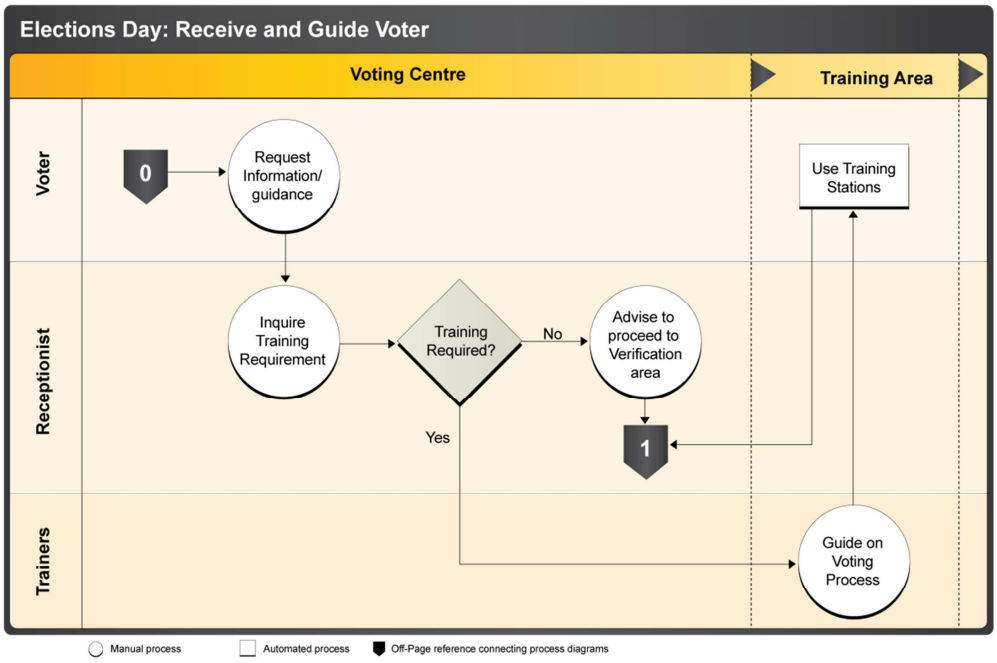


Figure A2-6: Voters' guidance procedures

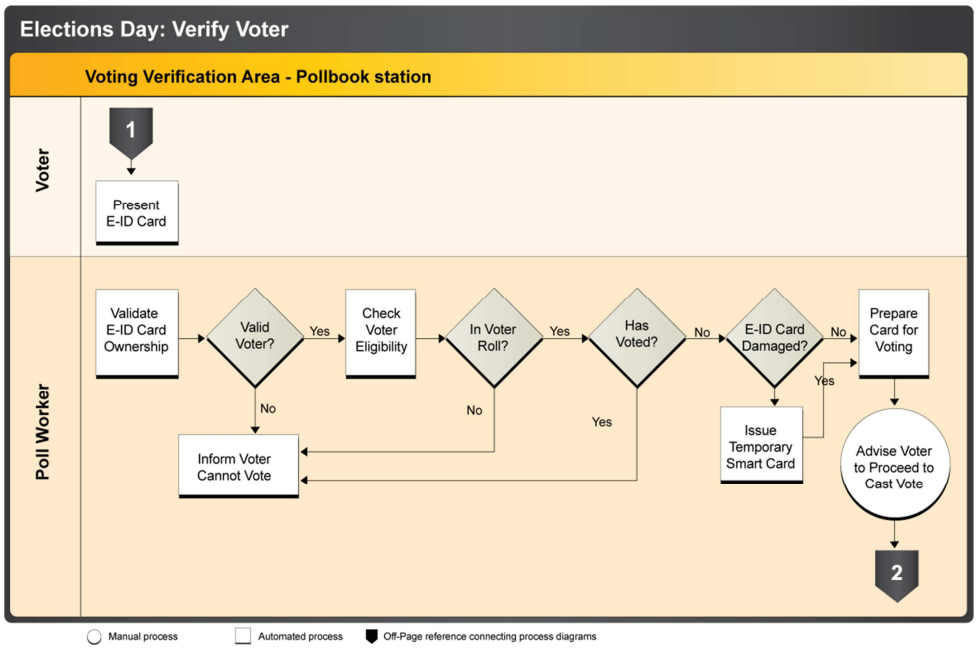


Figure A2-7: Voter's verification process

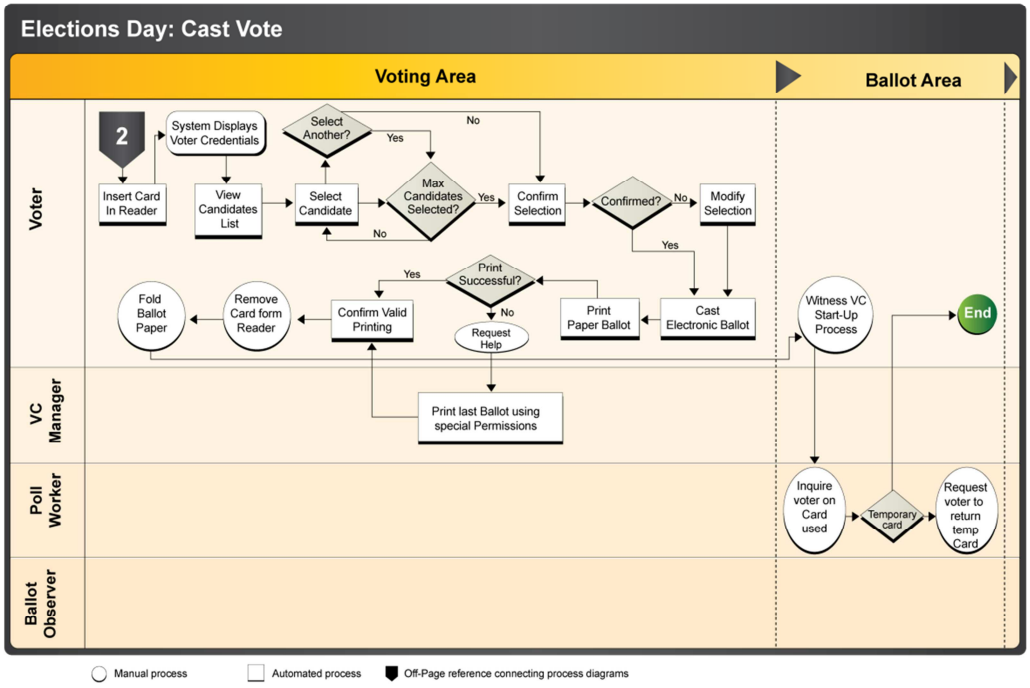


Figure A2-8: Vote casting process

A2-4.1 Process Steps (Election Date)
Process steps of Election Day has been separated in two identified areas: Voting Centres and Operations Centres.
In the voting centres

A2-4.1.1. Pre Opening Process
Input: poll worker user credentials
Output: voting terminals and servers are started and connected to central server
Pre-Requisites:

i) poll worker user credentials are available
ii) staff required to execute the process are assigned and available
iii) equipments required for electronic voting is deployed and tested in the voting centre

Table A2-4: Centre pre opening check process

Process Steps			
Steps	**Where**	**Who**	**Comments**
PRE-OPENING CHECK			
Before the voting centre is opened to voters, poll workers start up all the computers, etc. and **check again the connectivity**	Voting Centres	Poll workers Voting centre support team	• Mock Voting and / or zero vote verification could be done. • Electoral Board need to be present at the moment of initiating the process • Candidates or representative could be present as the Electoral Rule allow it

A2-4.1.2. Receive and Guide Voter Process

This process will be executed by voting centre Receptionists and does not involve the use of any automated system.

The Receptionists will be the first point of contact for the voter and will do the following

i) check if the Voter is carrying Emirates ID required for voting
ii) guide voter to training area, if requested by voter
iii) guide voter to Voter Verification area if voter is ready to vote
iv) provide general information on voting process, requested by voter

A2-4.1.3.Verify Voter Process

Input: Emirates Identity Card

Output:

i) Verified voter,
ii) Verified Emirates ID Card or temporary smart card prepared for voter to cast vote

Pre-Requisites:

i) Voter has Emirates ID Card
ii) Staff required to execute the process are assigned and available

Table A2-5: Voter authentication process

Process Steps			
Steps	**Where**	**Who**	**Comments**
VOTER AUTHENTICATION			
A voter gets into the voting centre and is addressed to one poll worker managing one pollbook	Voting Centres	Poll workers Voters	• Reception Area provide Customer Service if Required as First point of Contact • Training area also available if required
The poll-worker validates the identity and eligibility of the voter: • Checks the picture in the EIDA ID • In some cases, uses biometric authentication • Inserts the EIDA ID in the pollbook reader • The pollbook automatically checks the eligibility of the voter (he is in the electoral roll of this Emirate and has not voted before)	Voting Centres	Poll workers Voters	**Exceptions** Issue: What to do if the voter has not EIDA ID (but other ID document like a passport)? Solution:No Vote allowed. Electoral Rule **Issue:** What to do if no connectivity to data centre? **Solution:** Vote will proceed. Vote tobe stored locally until connectivity resumes. Then, votes stored locally will be synchronized with DC DB. **Note:** A special page showing connectivity logs/graphics, coupled with some dynamic green/red light showing on the header of the pollbook application will be available.
ISSUE TEMPORARY CARD			
If the voter has EIDA ID not readable (e.g. broken card), a blank card will be generated with a valid credential to vote.: • The poll worker search for the voter in the pollbook by typing his name and last name • The pollbook will tell whether the voter is able to vote or not • If the voter is eligible, the poll worker will issued a blank card to allow the voter to vote	Voting Centres	Poll workers Voters	• Pollbook functioning as credential issuing point

A2-4.1.4. Cast Vote Process

Input: Smart card with voter's credentials

Output: Printed copy of ballot to be placed in ballot box

Prerequisites:

i) Voter is eligible to vote

ii) e-Voting system is available to cast vote

Table A2-6: E-ballot voters cast process

Process Steps			
Steps	**Where**	**Who**	**Comments**
VOTER CAST E-BALLOT			
6. The voter accesses a voting terminal and logs in: • Inserts his EIDA ID in the terminal reader • Touches the screen to activate the process	Voting Centres	Voters	
7. The voter makes his selections if the authentication is correct • The terminal displays the candidates related to the voter's Emirate • The voter makes his selections • The voter clearly sees which candidate are the selected options • The voter presses "continue" button	Voting Centres	Voters	• Selection from 0 to the max number of candidates by Emirate • Blank Vote is allowed • Under-vote is allowed • Over-vote is **not allowed**
8. The terminal displays the voter a confirmation screen with the selected candidates: • The voter can go back to the previous screen and change his selection (previous step) • The voter confirms the selections by pressing the button "cast ballot" • The ballot is encrypted in the voting terminal and sent to the voting servers	Voting Centres	Voters	• Only selected candidates **(Name and Picture)** will be displayed.

Table A2-6: E-ballot voters cast process (cont.)

Process Steps			
Steps	**Where**	**Who**	**Comments**
PRIITING OF PAPER COPY			
9. The terminal shows confirmation of the correct storage of the ballot and instructions to the voter about the next steps: • Wait till Digital Ballot copy with selection is printed • Take the ballot copy • Voter confirms a valid ballot printing • Remove the e-ID card	Voting Centres	Voters	**Exceptions:** **Issue:** printer does not print the piece of paper **Solution:** the voter requests the help of a poll worker, who can access a special page and request a new printing by typing a special password.
10. The voting terminal returns to the initial stage waiting for a new voter • The voter is directed by poll workers to deposit his ballot copy in the ballot box. • This ballot box must be different to the one used to store any potential paper ballots cast. • The voter return the smart-card in case it was issued by the poll-worker.	Voting Centres	Poll workers Voters	• Special paper must be used for printing ballots which would allow to detect fake ones.
VOTER FINISHES			
11. The voter leaves the voting centre	Voting Centres	Voters	Business Owner to consider surveying voters about their experience

A2-4.1.5. In the operations centre

This is a resume of actions that can be done during Election Day in the operation centre:

Table A2-7: Monitoring Dashboard

Process Steps			
Steps	**Where**	**Who**	**Comments**
MONITORING			
12. Check the participation data in the dashboard	Operations Centre	Business Owner System Integrator Auditor	• Information displayed by Emirate
13. Check the status of the voting centres (whether they are connected or not)	Operations Centre	System Integrator Auditor Business Owner	• Each VC will periodically perform a service check against the data centre. • Dashboard will have an historic and graphics of each VC connectivity.
14. Check the availability/performance of the data centre equipment		Data Centre technicians	• This is responsibility of the provider of the Data Centre. • Probably it could be resolved by reports stating every two hours the status of the servers and the bandwidth.

After Election Day Process: Business Process Diagram

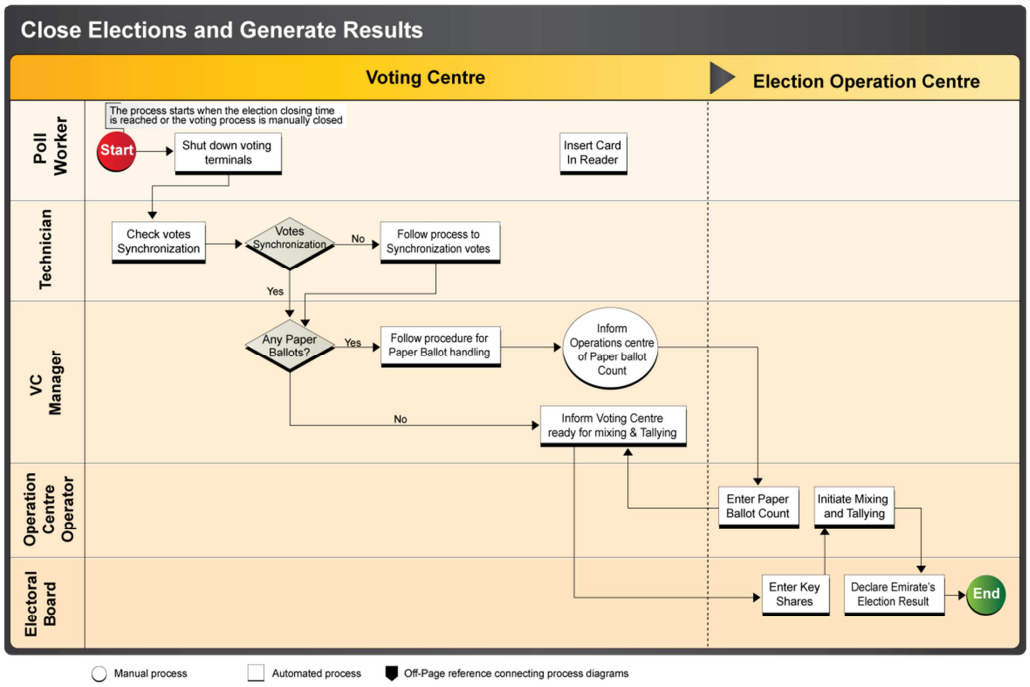


Figure A2-9: Closing elections and generating results process

A2-3 Process Steps (After Election Date)

Next are a short description of the steps to be done just after polls close an in the following days

A2-3.1 Close Elections and Generate Results process

Input: process is triggered automatically, once the pre-requisites are met.

Output: Votes counted and Elections result generated.

Pre-Requisites:

i) Elections is closed manually by VC manager or defined Election closing time is reached.

Table A2-8: Close Elections and Generate Results process - (1)

Process Steps

Steps	Where	Who	Comments
END OF VOTING PERIOD			
15. At the configured time (Date/ Time), the voting system will stop accepting ballots. Also, poll workers will not allow to access any voter to the voting centre.	Voting Centres	Poll workers	**Exceptions** **Issue:** voters still in the voting centre waiting to vote when closing time happens. **Solution:** (1) If the Emirate have more than one VC, then configure the voting system to automatically stop a few hours after the designated election closing time (e.g. 1-2 hours), and close the process manually when the voting centres report no more voters are present. (2) For those Emirates with only one voting centres in the Emirate then Election Admin board can extend the 'Election Closing time at their discretion'.
16. The poll workers will shut down all voting terminals and poll-books (log out and switch them off) • Operations Centre will be notified that the voting centre is "closed" for voting	Voting Centres	Poll workers	

Note: A documented procedure will be executed at each voting centre to close the election by not allowing any more votes to be cast including turning off the voting machines or stop the Pnyx server (side effect: synchronization to the data centre could still not be finished)

Table A2-8: Close Elections and Generate Results process - (2)

Process Steps

Steps	Where	Who	Comments
VALIDATE SYNCHRONIZATION			
17. The designated technician/poll worker will check in the local servers that all the ballots are synchronized with the central servers. • Notify operations centre of the checking result • Follow agreed procedure if some ballots are pending	Voting Centres	System Integrator Poll worker	Exception Issue: ballots pending synchronization Solution:Some options available: 1. Using a back up connection to finish synch 2. Export the data to a DVD and submit it manually to the operations centre.
PAPER BALLOT COUNTING			
18. If Paper Ballot was allowed, Poll workers will proceed to count paper ballots. • Break seal of ballot boxes • Manually count the paper ballots • Fill out report with results, usually signed by several poll workers. • Any other documentation and procedures associated to paper ballots handling will be followed	Voting Centres	Poll workers	**DEPENDENCY:** • NEC to define the procedure to manage/store paper ballots • The Form will be similar to the one used in voting Center and will be blank to be filled by an electoral officer. • After that this will be input into the Dashboard application
19. Local register of results to the Emirate operations centre • A representative of the voting centre will call the Emirate operations centre to report the results(in cases where the voting centre does not include Operations Centre). • An operator in the operations centre will record the results into the system	Voting Centres Operations Centre	Poll workers Operators	• It will be the dashboard where we will record the paper votes and later consolidate them with the results of the electronic votes.
DECRYPTION AND TABULATION OF E-VOTES			
20. When notified by all Voting Centres that they are ready (step above), and using a secure connection from the operations centre, the Electoral board in presence of the candidates attending the event, will authorize and initiate the Online Mixing and Tallying process.	Operations Centre	System Integrator Auditor Business Owner	**Exceptions** **Issue:** no connectivity with the data centre **Solution:** Mixing and Tallying process could be performed against local data base, since synchronization process keep all votes locally for contingency

Table A2-8: Close Elections and Generate Results process - (3)

Process Steps

Steps	Where	Who	Comments
21. The mixing/tabulation process can start: • The Electoral Board members insert, one by one, their cards to reconstruct the decryption key • The ballots are shuffled and randomly decrypted following a mixing cryptographic protocol • The results tabulated are displayed in the mixing server (number of votes per candidate). • Also, files with the decrypted ballots are exported from the server to be displayed.	Operations Centre	Business Owner System Integrator Auditor Electoral Board	• The results are also displayed in the Operation Room of each Emirate
RESULTS DISSEMINATION			
22. The results are uploaded in the WEB Result application for its public dissemination. These results shall include data from paper counting and electronic counting.	Operations Centre	Business Owner System Integrator Auditor	• The Final Results could be made public after the election (i.e. accessible by all the citizens) • We can import the elections and candidates also in dashboard using the CSV export file we have in Pnyx, so that we also have all election configuration in the Dashboard.
FINAL AUDITING			
23. Audit servers • The logical sealing of the different servers can be validated to see that they remain as before sealing. • Other logs can be validated too.	Operations Centre Data Centre?	Business Owner System Integrator Auditor	If VPN is open after election to the data centre, all validations can be done from the Operations Centre. This process can also be done before the mixing process, but it takes time and will delay the publishing of the results.

A2-3.2 Decommissioning of Equipments

Equipments at the voting centre shall be decommissioned and moved to designated sites, once elections are declared complete and closed.

Input: Instructions and authorization from NEC to start decommissioning

Output: Equipments decommissioned

Pre-Requisites:

i) All information on server is backed up and secured in the designated area

Table A2-9: Decommissioning of equipments

Process Steps			
Steps	**Where**	**Who**	**Comments**
24. Archiving the election data • The required data will be copied in WORM media (e.g. DVD) and delivered to NEC for its custody till the period open to claims is closed. This data should allow to redo a mixing/ tabulation process if required. After this period expires, the data can be destroyed. • Data in the servers related to ballots and voters should be removed	Several sites	Business Owner System Integrator Auditor	Pending to define which data is to be stored. Usually logs, ciphered ballots and mixing output, plus all configuration files and the Electoral Board and Administration cards.
ARCHIVING AND DECOMISSIONING			
25. Audit paper copies of ballots, if required.	Voting Centres	Poll workers Business Owner	Manual process, and probably only done on a fraction of the ballots and/or in a single voting centre.
26. Decommissioning of all the equipment: • Voting centres • Operations centre	Each voting centre Operations centre	System Integrator Business Owner	

A2-5 Contingencies to the Business Process Exceptions

A2-5.1 Exceptional process

Next, we will represent some exceptional process diagrams correspondent to equivalent situation foreseen in the voting process.

A2-5.2 Ballot printing fails

- Ballot copy is required to be printed and stored in Ballot box for auditing purposes
- If printer fails, Voter should request assistance from Voter Centre Officer to authorize the reprinting process
- Only three attempts will be authorized by the system.
- Below is the Process diagram representing this exceptional process

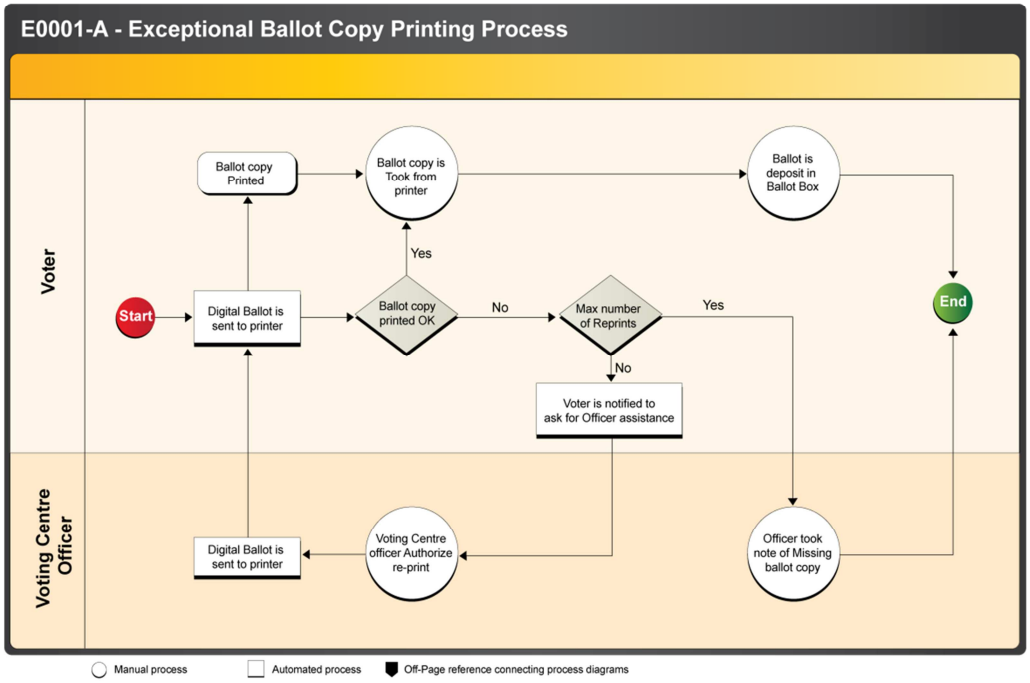


Figure A2-10: Exceptional ballot copy printing process