Elections and Technology

The introduction of information and communications technologies (ICT) into the electoral process is generating both interest and concern among voters, as well as practitioners across the globe. Today, most electoral management bodies (EMBs) around the world use new technologies with the aim of improving the electoral process. These technologies range from the use of basic office automation tools such as word processing and spreadsheets to more sophisticated data processing tools, such as data base management systems, optical scanning and geographic information systems.

While these technologies open up new frontiers and offer new possibilities for the electoral process, especially for voting operations, there may be unforeseen risks involved, such as an increase in vote selling or difficulty in auditing election results. Careful consideration also needs to be given to the risks of inappropriate or untimely introduction of technology, especially if it has the potential to compromise transparency, local ownership or sustainability of the electoral process.

Introduction

Overview

Why "Elections and Technology"?

In many countries, technology is present in activities related to the electoral process, and in some cases it is essential to the conduct of elections. Technology is used, for example, to compile voter lists, to draw electoral boundaries, to manage and train staff, to print ballots, to conduct voter education campaigns, to record cast votes, to count and consolidate vote results and to publish election results. The appropriate application of technology to elections can increase administrative efficiency, reduce long-term costs and enhance political transparency.

Technologies used for elections can include familiar and older ones like printing presses, ball point pens, manual typewriters, electronic calculators and radios, or newer technologies like computers, optical scanners, digital mapping and the Internet. The logistics of modern large-scale elections can be a considerable challenge for countries without access to technology.

The complexity level of technology used for the administration of elections around the world varies enormously. The rate of technological change is so high that election management bodies (EMBs) must regularly re-evaluate their use of technology to determine whether they should adopt new or updated technology to improve their performance.

This Elections and Technology (ET) topic area aims to assist EMBs in this task by:

- describing technologies that are currently being used for electoral processes
- presenting guidelines for the evaluation, choice and implementation of new technologies
- providing examples of so-called best practices in the use of technology as well as examples where technology has not lived up to expectations
- examining some of the emerging technologies and trends to identify those that may apply to elections in the near future

The ET topic area is different from the other topic areas included in the Administration and Cost of Elections (ACE) Project. While the other topic areas cover specific aspects of the election process, the ET topic area covers technology appropriate to those topic areas.

The use of technology in elections is not an end in itself, but assists in the various aspects of electoral administration. For example, electronic database management systems can be used in several components of the election process, such as voter lists, material inventories, personnel management, payroll, election results dissemination and statistics.

To relate the use of technology to specific election processes, the ET topic area contains links to relevant topic areas on the ACE Project website and to the Internet.

The meaning of "technology"

“Technology” can be defined as anything involving the application of science and engineering. This broad definition can cover any manufactured item, so a more limited definition is adopted to consider items directly relevant to election administration.

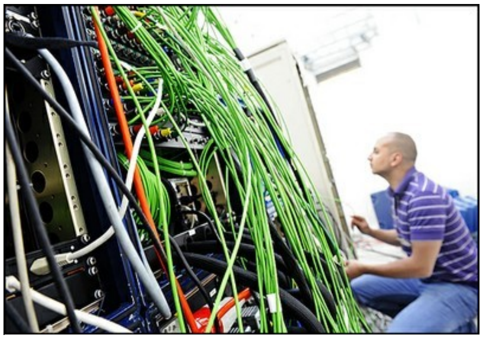
“New technology” can mean new in one place and old in another, in addition to being an evolving concept. The Gutenberg printing press, wristwatches, manual typewriters and ball point pens were once considered new technology when they were developed, but in the 21st century they are hardly thought of as technology.

"Elections and technology" often refers to software programs and electronic equipment, such as computers, printers, scanners, bar code readers and the Internet. But there are other technologies used in elections that do not directly involve computers, but rather new materials, such as cardboard, fibreglass and plastic used in polling equipment.

Within this topic area “technology” may refer to existing or so-called old technology, as well as emerging or developing technology. It may include computer hardware and software, other electronic equipment, mechanical devices and some materials. References might also be made to non-electronic innovations and techniques with specific electoral applications.

The main focus is on practical issues such as the type of technologies that are currently in use around the world and guidelines for the implementation and maintenance of technologies.

Implementing technology for election administration



On the process of implementing specific technologies for elections administration, there are a few considerations to take into account, some common to any implementation of technologies others more specific to the electoral process:

Elections can be a high risk activity . They have to be conducted properly, open to public scrutiny, and there is not much room for errors. Unlike other applications of technology, where systems can be introduced gradually with extended testing and implementation schedules, many election systems are used for the first time on Election Day and, therefore, must work correctly or the entire election may be jeopardized.

An electoral management body needs to consider the upgrade of existing technology versus the introduction of new technology. Thorough evaluations are necessary to avoid incurring high costs for relatively minor improvements. Depending on the application, it may be more appropriate to continue using the existing system.

This leads to the consideration of the cost-effectiveness of implementing a new technology. Evaluation studies of costs and savings associated with introducing technology need to take into consideration, not only the initial costs involved in purchasing equipment and materials, but also the cost of setting up the new system, additional expertise and the need for ongoing maintenance and management. (This will likely involve obtaining an additional commitment of funds through the relevant government budgetary process.)

Another consideration is the sustainability of technologies under evaluation. [In most applications, there is a need to ensure that the technology adopted can be used during extended periods covering several elections. Adopting technologies that can become quickly obsolete or unusable may prove expensive and unsustainable in the long-term.

Some technologies are changing at such rapid rates that it is almost impossible to avoid short-term obsolescence. In this case, it is important to study existent technology standards and trends in order to adopt protective measures that can decrease both the impact of future versions or systems and technical incompatibilities. Personal computer processing power is a good example of how "state-of-the-art" technology can rapidly become obsolete and therefore how important it is to choose suppliers that ensure upward compatibility that will facilitate the smooth transfer of data from an old to a new computer. In addition, other alternatives such as leasing equipment rather than purchasing, might be considered to optimize the use of resources.

To determine the appropriateness of implementing new systems with new technologies, other factors such as the local physical environment and infrastructure need to be considered. A country with an intermittent power supply, for example, may not be an appropriate location for implementing a wide area network of personal computers that require a reliable power source. High humidity or high levels of dust or sand may also restrict the choice of appropriate technology.

Security issues are also involved. Particularly for systems used for recording, tallying or transmitting voting data, the technology must ensure the security of the data as well, if not better, than the equivalent manual processes that are being replaced.

Before new technologies are introduced, it is important to consult with all of the stakeholders who are likely to be affected. EMB staff must be willing and able to implement the changes.

Participants in the election process such as political parties, candidates, members of parliament and the media need to be consulted if the change affects them as, for example, in a case where an electronic voting system is being considered. New technology may also require changes to the relevant electoral laws and rules, which means that these changes need to be negotiated and guaranteed before a commitment to the new technology is made.

Time frames for implementing new technology need to be carefully studied and defined:

- to consult with stakeholders
- to identify and evaluate needs
- to evaluate and select specific technology to be adopted
- to implement the new system
- to test the system features and outcomes in order to make sure that it works properly when needed
- to train the users of the system

It is common for EMBs to underestimate how long it takes to implement a new system. And yet, if not enough time is allocated to implementing the new system or if implementation is rushed, even though the system may be considered ready at election time, there is an increased risk that one of its crucial steps will fail. (In the late 90s elections were cancelled in a Latin American country on the day of elections because the new voting system was not ready.)

Another potential pitfall is attempting to do too much too quickly. If possible, it is better to introduce new technologies gradually, even over a series of electoral events, instead of trying to implement new technology all at once, in a single step.

Once a decision on a new system is taken, an implementation plan needs to be developed with expected outcomes, timelines, allocation of responsibilities, checklists, standards, quality controls, training of support staff, training of users and an implementation budget. If possible, it may be useful to undertake a pilot program first, to test the new system on a small scale.

After the successful testing of pilot systems, preparations for a full-scale system implementation can start, including a “load test” where the system is tested by conducting a mock exercise that is as close as possible to the real situation.

Another essential step for the successful implementation of a system using new technologies is to determine who is going to use the system and in what capacity, in order to organize appropriate training sessions. In the case of systems used only by EMB staff, for instance, it may be necessary to only train related staff. Where the system is used by EMB staff and outsiders, different training sessions might be needed; one adapted to the staff and another to the outsiders. For example, if an electronic voting system is introduced, EMB staff may have to be trained as trainers who, in turn, train polling workers to assist voters. In addition, a massive communications campaign might be organized to prepare voters to handle the new system and technology. Time for conducting user training has to be built into the implementation plan.

Then come the risks: any technology, new or old, can fail. When new technologies are first implemented, the risk of failure can be higher than with tried and tested systems.

Consequently, it is important to have in place contingency plans. Often this involves setting up manual back-up systems that can kick into operation at short notice whenever the technology fails. For example, where ballots are being counted electronically, plans have to be in place to enable a switch to a manual count whenever the electronic system fails. Computer systems also have to be designed with appropriate back-up systems, such as the use of mirrored servers, automation of back-up copies of data and off-site facilities to regularly store copies of data.

What types of technology will be covered in this topic area?

If an EMB is considering the use of new technology for election purposes, it might want to start by looking at technology currently in use for similar purposes, who is using it and what issues have arisen in its use. The Elections and Technology topic area looks at three main categories of technologies, with sub-categories, currently in use around the world:

- Communications: Telecommunications, Radio, Networks and the Internet.
- Computer Hardware and Software: Word Processing, Spreadsheets, Database Management Systems.
- Other technologies: Specialized Electronic and Mechanical Devices, Non-electronic Innovations and Materials.

This is followed by a review of technologies used within specific electoral administration, such as:

- Boundary Administration
- Technology for Voter Registration
- Technology for Regulation of Party and Candidates
- Technology for Reaching Voters
- Technology for Voting Operations
- Technology for Corporate Management

The ET topic area also looks at issues related to the use of technology, such as management of technology and trends that may affect the future use of technology in elections.

Image:

Guiding Principles

Whenever an electoral management body (EMB) considers the use of technology to facilitate and improve the electoral process, it is advisable to follow several guiding principles that have been identified over the years and that can help to establish and maintain public confidence in the electoral process.

These guiding principles are:

- take a holistic view of the new technology
- consider the impact of introducing new technologies
- maintain transparency and ensure ethical behaviour while adopting new technology
- consider the security issues related to the new technology
- test the accuracy of results produced by the use of technology
- ensure privacy
- ensure inclusiveness
- consider the technology cost-effectiveness
- evaluate efficiency
- evaluate sustainability
- evaluate the flexibility of the technology to adapt to new election regulations
- consider the service provided to the users and their trust in the new technology

Take a holistic view of the new technology

Technology is just a tool and therefore it is not an end in itself. When technology is applied to any activity related to electoral administration and elections, it is important to consider carefully the electoral context in which the technology is used. For example, if technology is being considered for vote counting, the guiding principles that apply to vote counting also apply to the technology.

It is also good to keep in mind that electoral processes involve more than just operations and technology. They include relevant laws, regulations and guidelines, social and political context, organisational culture, procedures developed to complement the technology and training of technicians and users.

Consider the impact of introducing new technologies

When a new system is being considered to replace another, an evaluation is needed to assess the impact of the change on all stakeholders.

Once the system is adopted, the transition phase needs to be carefully managed to ensure that problems do not occur and that all functions can continue to be effectively carried out.

These are some strategies that can be used by electoral administrators to minimize the impact of new systems, new technology and changes on electoral processes:

- Allow plenty of time for implementation and avoid startingavoid starting implementation too close to Election Day.
- Keep in mind that implementation of a new project often takes longer than expected.
- Plan for new systems to be finished well before the earliest practicable election date and enforce cut off dates after which no system changes are allowed.
- Have alternatives ready to be implemented in case the new system cannot be used for whatever reason.
- Manage information about the technology and changes so that stakeholders do not have unrealistic expectations and do not impose impossible deadlines.
- Avoid imposing a new, untried or unsuitable technology.
- Schedule enough time to thoroughly test new systems.
- Provide training for staff and users as needed.

A system implementation schedule can be influenced by whether there is fixed term or variable term election systems. With fixed term elections, implementation schedules can be set around a known election date while with variable term elections, new systems should ideally be in place and ready to go before the earliest likely date for the election.

Maintain transparency and ensure ethical behaviour while adopting new technology

Transparency, meaning openness and accountability, is a key feature for the credibility of democratic elections. An indicator of transparency can be the access by electoral observers, both domestic and international, to all procedures at every stage of the electoral process.

With manual processes, transparency is relatively straightforward, as the processes are usually visible and it is not difficult to provide meaningful access to observers. By contrast, with the use of some technologies it may be more difficult or even impossible for observers to testify that the outcome is correct. Electronic voting systems are one example where in some cases it is almost impossible to insure that the vote that is registered is indeed the vote cast by the voter and, therefore, that the resulting vote counting is accurate. On the other hand, the use of technology may enhance transparency once the data entry into the respective system is proved to be accurate and large quantities of data can produce meaningful reports with very few errors.

With the use of technologies, transparency may have to be provided in completely different ways depending on the technology. This may involve the use of techniques, such as creation of audit trails, creation of log files, code verifications, digital signatures and compilation checks, among others.

As a result, the skills needed by observers of electoral processes using various technologies, may be completely different than those needed to observe manual processes. To ensure transparency, the election management body may seek the assistance of specialized experts or auditors able to verify the accuracy of their systems and to provide special training to observers.

Related to the issues of transparency and trust, EMBs are expected to follow appropriate ethics when implementing new technology. For instance, when choosing technology suppliers, EMBs are supposed to ensure that the tendering processes are fair and open, without favouritism or corruption and that all government purchasing procedures applicable to the selection of technology are followed.

When buying hardware and software, EMBs have to ensure that proper licences are obtained. Apart from the legal and ethical problems with using unlicensed or unregistered software, users also run the risk of not being notified of known bugs, software fixes or upgrades.

Consider the security issues related to the new technology

Computer systems used for elections must include high levels of security. Unauthorised persons must be prevented from accessing, altering or downloading sensitive electoral data. Demonstrable security levels are another way of ensuring that election systems are transparent and trustworthy.

Various mechanisms exist to provide for computer security. These include password protection, encryption, verification programs and physical isolation.

Test the accuracy of results produced by the use of technology

Accuracy is vital to the credibility of an election, particularly voters' lists, vote recording, vote counting and the reporting of election results. To ensure that technological systems are trustworthy, there must be ways to test and verify that data is recorded properly and that the manipulation of this data produces accurate outputs.

System accuracy may be tested by randomly entering known data into the system and verifying that the resulting outputs are correct. In addition, for voting systems, a test is supposed to be performed to verify that the same set of data processed through several randomly chosen, similar but independent systems produces the same results.

On the whole, it would be expected that accuracy would increase as new and improved technology was adopted.

Ensure privacy

Electoral computer systems often contain sensitive personal data on large numbers of individuals, which can include names, addresses and other personal details. While many countries have privacy laws and policies that place restrictions on access to personal information, as a general principle, every person has the right to personal privacy. If a person's privacy is invaded by improper use of electoral data, both the person and the respect accorded to the electoral process may suffer.

Accordingly, security built into electoral computer systems should take account of the need to protect the privacy of personal data held on them. Audit trails can be built into systems containing personal data to track and monitor which individuals have accessed or modified personal data and to prevent any unauthorised invasion of privacy.

Ensure inclusiveness

Where a technology with impact on internal and/or external users is being adopted, it is advisable to organize a consultation process with those users or their representatives to ensure that their needs are met and that they are satisfied that the new system is acceptable and reliable. It is important to provide sufficient information to users to enable them to feel included in the process and therefore increase the likelihood that the new technology will be successfully implemented.

Since election technology has the potential to directly affect the political process, it is important to engender a sense of ownership in its users, much more so than might be considered for other government systems.

In addition, access and equity considerations are to be taken into account when adopting new technology to ensure that people with special needs are included.

Consider the technology cost-effectiveness

Depending on the application, the use of technology may imply a substantial upfront investment, even if the benefits are considerable and possible long-term savings can outweigh the initial cost. In addition, relatively low-cost technology can also replace high cost, low-tech processes, leading to savings in the long-term. Costs with ongoing maintenance also need to be considered and may be much higher than expected.

Therefore, before making a commitment to implement new technology, it is important to determine whether it is financially viable by getting a complete account of all likely costs and savings, namely:

- basic up-front costs of the technology itself
- expected costs with add-on equipment such as peripherals and communications
- installation and implementation costs
- expected on-going troubleshooting and maintenance (addition of new features, and performance and capacity optimization) costs over system life span
- expected costs of warehousing related equipment
- expected costs related to documentation, design of new procedures, staff training and user training
- expected financial benefits from increased efficiency
- comparative costs of other available technologies that offer the same functionality

In addition, the following related studies might also prove useful:

- cost-benefit survey
- assessment of expected improvements in efficiency or service versus extra costs
- likelihood of funding during the project life span
- evaluation of likelihood of sharing the new system and related maintenance costs with other agencies or organizations
- assessment of the opportunity for joint ventures that could reduce costs without compromising integrity
- evaluation of similar solutions, if they exist, implemented by either other election management bodies or other organizations

These considerations and the results of these studies can help to identify additional functions, benefits and user satisfaction to be provided by a technology under investigation. These considerations can also help to provide a realistic estimate of expected costs or savings needed for a thorough evaluation of a technology’s cost /efficiency ratio. This, in turn, can help determine whether the technology is worthwhile, viable and affordable.

Relatively minor improvements may not justify the extra cost and by the same token, if a low-cost, low-tech solution is available and it is acceptable for the specific task, there may not be a need to implement a proposed high-cost, high-tech solution.

Whenever possible, the expected life-span of the technology is also supposed to be determined. In principle, a technology that can be re-used for more than one purpose or for more than one election is more cost-effective than one that can only be used once before it needs to be replaced.

In addition, before accepting a technology purchase, there is a need to ensure that there are available funds to cover implementation costs as well as ongoing maintenance. Generally this implies commitments through the relevant government budgetary process.

Evaluate efficiency

Although it is often expected that a new technology is more efficient than the old one, it might not be the case in practice. It is possible to replace an efficient manual process with an inefficient automated one if the new process is not carefully thought through. When deciding to implement a new technology, it is important to ensure that the new system is more efficient than the one it replaces.

One of the anticipated benefits of technology is the ability to perform accurately large complex tasks in a relatively short time compared to the time needed to undertake the tasks manually. While this may enable EMBs to reduce costs by deploying fewer staff, it may also lead to additional pressure on staff as productivity rises and more is expected of them.

Evaluate sustainability

Technology is generally expensive to acquire, but if it is sustainable, and able to be used for more than one purpose or more than one election, it can be more cost-effective in the long term.

New technology may also require the use or availability of other technologies or specific infrastructures, such as communications and electrical energy networks. For example, if a country has an intermittent power supply, implementing a network of personal computers may not be the best choice. High humidity or high levels of dust or sand may also restrict the choice of appropriate technology.

In general, local infrastructure must be capable of supporting a chosen technology. If it is not, it could mean that the technology being considered is not appropriate or that there is a need to upgrade the infrastructure, in which case costs and benefits should be carefully assessed.

There is also a need to evaluate the technical and financial capacity of the electoral management body (EMB) to maintain a new system during an agreed upon or required time span. Usually, it is desirable for an adopted technology to be used for several years; therefore funds will need to be secured, not only for initial implementation, but also for the foreseeable life of the technology. These funds need to be budgeted for and guaranteed before committing to a new technology.

Another aspect related to the sustainability of a new system is the availability of appropriately skilled staff to run and maintain it, either by the EMB or by outside service providers. The costs associated with keeping staff skills up-to-date and the capacity of both EMB and service providers to retain trained staff need to also be considered.

Another potential pitfall is attempting to do too much too quickly. Instead of implementing a radically new technology (compared to the existing local technology) in one step, it may be more appropriate to gradually implement change over a series of electoral events.

Evaluate the flexibility of the technology to adapt to new election regulations

A technology that is flexible is also more likely to be cost-effective and sustainable. It may be desirable to adopt a technology that has the potential for more than one use if this does not compromise the primary need for the technology.

In cases of transitional environments, where the future of election management methods is uncertain, it is desirable to avoid purchasing technology that is highly specialised and inflexible, and to purchase instead more generic products that can facilitate the use of a wide range of applications.

Another of the perceived advantages of using technology for elections is its ability to provide users with greater flexibility and more options. Therefore, procedures may be implemented to ensure that the new technology does not reduce flexibility by limiting the number of options available. For example, it may be more desirable to introduce electronic voting as another option to using manual ballots, rather than completely replacing manual ballots with electronic voting, to ensure that users without electronic skills or access are not disadvantaged.

Consider the service provided to the users by the technology

Elections are largely about providing a service for its clients, the voters. When choosing a new technology, the level of client service—ease of use and voters' satisfaction—as well as how the technology is perceived by its users needs to be a priority consideration for the EMB in order to ensure that the credibility of the electoral process is not jeopardized.

There are a number of strategies that can be adopted to reduce users' unrealistic expectations or suspicion and ensure trust:

- assessment of stakeholder receptivity to review specific technologies
- clear definition of technology objectives

- use of open and regular consultation process with all relevant stakeholders
- verification of legal implications of adopting a specific technology
- use of rigorous technology evaluation processes including need for and implementation risks
- provision of appropriate levels of security for the electoral process different tasks
- verification of funds availability to cover all implementation, maintenance and training costs
- setting up transparent tendering and purchasing processes accepted by all stakeholders
- organization of effective training strategies both to electoral administrators and users
- assessment of references, use of external audits and verification checks to assert the trustworthiness of external vendors, technical staff, software programmers and consultants involved in supplying and/or maintaining technology

Besides a rigorous and well-structured implementation process, the successful adoption of a new technology requires the acceptance, trust and satisfaction of its users.

Context

The context in which a technology is applied is an important consideration. This is particularly true when choosing a new technology for electoral processes, where additional factors such as political and social issues can prevail over technological ones.

As different technologies are made available, electoral management bodies (EMBs) evaluate not only their usefulness in performing tasks related to electoral administration but also the impact they can have on the citizens. As a result, there are technologies specific to office automation and accounting that are used by EMBs for administration and management issues. Other technologies, such as those specific to voter registration and voting systems have a direct impact on the way citizens perceive the overall electoral process.

In addition, not all countries evaluate a new technology in the same way. Different countries choose different technologies and adapt them to their specific election systems. A technology trusted by one country may be completely mistrusted by another due to different political, social and cultural contexts.

This means that when an EMB is evaluating a technology for use in its country’s electoral administration, and particularly in its voting operations, it needs to be sensitive to the country’s social, cultural and political environment. Depending on the environment—for example, when a society is in political transition—people may either expect more from a specific technology than it can realistically deliver or be suspicious of the use of a new technology.

Political opposition to innovation or change is also possible. Elections by nature are politically sensitive, and the implementation of a new technology may have a political impact. When political parties and voters distrust a technology, there can be delays in implementing a project or it may be halted altogether. For example, introducing Internet or telephone voting may increase access to voting facilities, but it may also increase suspicion of fraud and vote buying.

There may also be bureaucratic opposition to innovation or change, especially when there are vested interests in retaining the current system. Adoption of technology often changes the nature of a workplace—without necessarily reducing the workforce—by changing the needs for specific skills.

Proposed changes in technology may also be subject to public inquiries, which are a good way to gauge citizen reaction and generate media interest. EMBs effective cooperation with public inquiries and independent evaluations at an early stage of the process is likely to promote trust and understanding among all stakeholders.

Security

Security also has an impact on the likely success of the electoral process particularly when a country is in transition to democracy. If there is a risk that an election process may be disrupted by civil unrest or sabotage, the technology chosen must be robust and flexible enough to function, even if part of the system becomes inoperable. This may involve employing strategies such as maintaining multiple backups of data at several different sites or ensuring that networks can operate even when one or more links are down. It may be best to have manual back up systems available to be used in the event of unrecoverable system failure.

Legislative framework

Depending on electoral systems and the legal instruments that regulate elections, there may be restrictions on the adoption of new technology and on the way it is procured. Therefore there may be a need to request a review of those legal instruments before the adoption of such technology.

In addition, specific government regulations may impact the adoption of technology by:

- limiting procurement of goods by type or place of manufacture

- limiting the type of applications that may be developed, implemented and maintained in-house and/or those requiring various functions to be outsourced
- requiring technology purchases to be vetted or approved by appropriate authorities external to the election management body (EMB)
- requiring that purchased hardware or software is compatible with those used by other government agencies to facilitate integration of data, if needed
- setting minimum standards and quality controls to be followed when implementing new systems

This means that the applicable regulatory environment may have a significant impact on the implementation of technology by the electoral administration bodies. Any standards and restrictions on technology acquisition needs to be identified early on in the planning stages to avoid conflicts and to ensure not only that appropriate technology is considered and adopted, but also that the implementation process can take place smoothly.

Implementation of digital voter registration systems and use of electronic voting systems, for instance, usually implies change of the legislative and regulatory framework.

If needed, legislative changes are supposed to have been approved prior to commitment of funds to develop and implement new systems and new technologies.

Since legislation can have a significant impact on the type of technology that can be used for an electoral process, it is advisable to request legislators to use language that allows some flexibility in the choice of technology by the Electoral Management Bodies.

Historical review

Elections as we know them today date from electoral processes developed in the mid- to late 1800s in the world's then fledgling democracies. At that time several new electoral concepts were introduced. One was the secret ballot, which required an anonymous voting interface, usually a printed ballot paper. Another was the gradual extension of the franchise—eventually to near-universal suffrage—requiring an authority to keep printed records of the names of eligible electors. The extension of the franchise, in turn, created the need to manage a process of communicating with, and taking and counting the votes of, the great majority of the adult population.

The history of the use of technology for elections is concerned with meeting these three needs — a voting interface, a list of eligible electors and the management of the voting process.

In the 1800s these needs were met using the available technology of the day, including printing presses and writing implements, such as steel-nib pens, fountain pens and, in the late 1800s, typewriters. However, most processes were then (and in some places still are today) manual. Electoral rolls were written by hand or manually typed, and kept in books and on cards. Ballot papers were distributed, marked and counted manually. Election results were manually calculated and communicated by tally board and print.

The mid- to late 1800s marked the beginning of a technological revolution that has continued to this day. As technology advanced, electoral management bodies (EMBs) applied the various innovations to electoral management.

The invention of electricity and the development of power stations led to electric typewriters, more efficient printing processes, and electronic voting devices and, eventually, computers, in addition to all those other lifestyle benefits we now take for granted, such as better-lit and better-heated workplaces. The invention of the internal combustion engine revolutionised transport, making rapid movement of large quantities of material and personnel possible on an unprecedented scale.

The development of mass communication techniques that took place in the 1900s also had electoral implications. Sound and vision recording and transmission, leading to radio, television, telephones, facsimiles, audio tapes, video tapes, compact discs and the Internet, have all been used for electoral purposes.

While these technological innovations gradually improved the management of the electoral process from the 1800s to the mid-1900s, it took the development of the computer to revolutionize it.

Today's computers were inspired by punch-card tabulating machines invented in the late 1800s. These in turn were inspired by punch-card weaving systems, first invented in 1801 by Joseph Marie Jacquard, a French weaver.

The first modern electronic computers were developed in the 1940s and 1950s, to the point where they became commercially viable. One of the earliest electoral uses of a computer was the tabulation of the election results for the 1952 United States presidential election.

By the 1960s many large businesses relied on computers. While the development and use of transistors and integrated circuits had by then shrunk computers from the giant valve-based prototypes of the 1950s, it took the development of the personal computer in the 1970s to make computers accessible to large numbers of users. A parallel advance was the development of user-friendly computer programming, or software, putting the power of computing in the hands of the general user. As advances in computer design continued at an accelerated rate through the 1980s and 1990s, computers became an indispensable part of life in developed countries around the world, both at work and at home.

From their beginning as relatively simple automatic calculating machines, computers today are capable of a huge range of functions, including statistical tabulation and analysis, data collection, storage and manipulation, electronic publishing and printing, word processing, communication and entertainment.

Computers did not begin to have a significant impact on election management until the 1970s and 1980s. With the exception of the use of mechanical voting machines in the United States, up until the 1970s most election processes still relied on the use of printed ballot papers and laboriously compiled hand-written or typed electoral rolls.

In the 1970s and 1980s, the increasing use of computers in business, first the large main-frame computers, and then the smaller more affordable personal computers, led to more and more use of computers for electoral applications. Early uses included election result tabulation, and electronic storage and retrieval of electoral roll data. As computer systems developed further, electoral uses kept pace, so that computers are today used for virtually every part of the election process in some parts of the world.

Most technological applications that have electoral uses are general in nature, and can be used for many different tasks beyond election management. That said there is at least one branch of technology that is election specific: mechanical or electronic voting machines. These have largely been confined to elections in the United States.

The first mechanical voting machines used levers to turn counting wheels. The first official use of a lever type voting machine was in Lockport, New York in 1892. Their use was gradually extended, and by 1930, lever machines had been installed in almost every major city in the United States. By the 1960s over half of the votes in the United States were cast on lever machines.

Another type of mechanical voting machine was the punch-card machine, developed in the 1950s and 1960s. Voters used a supplied device to punch holes opposite their preferred candidates' names on the ballot cards. After the polls closed, the results were tabulated by mechanical card counters.

Optical scanning voting systems were developed in the 1970s. Voters make marks on paper ballots to indicate their choice of candidates. A scanning device then reads the marked entries to calculate the results.

In the 1990s, advances in computer technology led to the introduction of Direct Recording Electronic (DRE) voting systems. These systems allow the voter to directly record votes using a computerised ballot display provided via mechanical or electro-optical devices. Once the voter has made his or her ballot selections, the device processes the data with a computer program and records voting data and ballot images into internal memory devices that are used to tabulate the results.

By 1996, over 98 percent of the ballots in the United States' local and presidential elections were cast using one of these mechanical or electronic methods.

Beginning in the 1990s the telephone was also used as a type of DRE voting system. Voters were able to record their votes directly into computer systems using the key pad on the telephone. They could identify themselves with Personal Identity Numbers (PINs) and record their choices by following recorded messages.

By the end of the 1990s the Internet ushered in a new medium for voting. Again, the United States led the way in electoral technological innovations, when Internet voting was used for the presidential primary elections in 2000.

It is important to note that today, different parts of the world are on vastly different points of the technology continuum. The level of sophistication of technological applications for elections varies widely from country to country. While electronic and mechanical voting systems are commonplace in the United States and in some Asian, South American and European countries, and computers are used for general election management in many developed countries, many less developed countries still conduct elections using manual techniques similar to those used in the 1800s.

Technologies with Electoral Applications

An election is a complex, multi-faceted event happening on a given date and subject to precise laws and regulations. The entire process is organised by an electoral management body (EMB). Each country structures and names EMBs in a variety of ways, but their responsibilities are similar. To fulfil their roles and mandates, an EMB needs staff, equipment and funding.

EMB responsibilities include:

- securing and providing electoral equipment
- the design, procurement, purchase, storage, distribution and eventual recollection of voting materials
- the recruitment, administration, training and

deployment of personnel to the voting places

- counting, tabulating and reporting votes recorded on ballot papers or voting machines and providing information to voters

Depending on the electoral system and applicable legislation, an EMB might organise and plan the voters' registration as well as the registration of political parties and candidate.

Several technologies are available to assist EMBs, including telecommunications technology, computer hardware and computer software, among others.

Telecommunications technology refers to telephone, radio, television, wireless and satellite communications as well as computer networks and the Internet.

Computer hardware and software include computing devices, open source and proprietary office automation aids such as word processing, spreadsheets, databases and multi-purpose programming tools. Open source is software that can be freely obtained or downloaded and involves minimal or no annual maintenance costs. There may be, however, development and management costs. Proprietary software often requires an initial acquisition fee, correlated to usage and an annual maintenance fee.

Other groups of technologies include devices such as counting machines, mail sorters, printers, projectors and screens.

Technologies for specific electoral tasks, such as boundary delimitation, voter registration, regulation of party and candidates, reaching voters, voting operations and corporate management are considered separately in this topic area.

The discussed technologies include among others, electronic and mechanical voting systems, scanning systems, identification systems, the Internet and office automation.

Electronic and mechanical voting systems

There are different types of electronic and mechanical voting systems. Some use technologies developed specifically for electoral purposes. Mechanical voting machines were used widely in the United States, and to a lesser extent in a small number of other countries around the world, but are being replaced by electronic voting machines. Different electoral electronic devices are already in use in several countries and their use is expected to increase.

The main types of electronic voting systems include:

- punch card voting/tabulation systems
- machine readable (optical scanning) voting/tabulation systems
- direct recording electronic systems

Scanning

Electronic scanning systems are used to convert data marked manually on paper into electronic form. While scanning is often used to capture voting data written into machine-readable ballots, it can also be used to capture other data, such as lists of electors who have voted or information shown on forms.

There are four main types of optical scanning technologies:

- optical mark reading (OMR)
- optical character recognition (OCR)
- intelligent character recognition (ICR)
- imaging technology

Identification systems

Several stages in the election process need to reliably identify a person: when a person votes, when a person registers to vote or when an employee needs access to a restricted place.

Some countries rely on the voter's self identification, without the need of an electoral identification document. Other countries may require specific electoral identification system.

As electronic voting becomes more widespread and more automated, particularly where voting is introduced on the Internet or by telephone, these identification systems become crucial to ensure that only eligible voters are able to vote.

There are different types of identification systems:

- identity cards
- personal identity numbers (PINs)
- bio-identification systems (including voice, hand, finger/thumb, retinal identification systems)
- digitised photography
- bar coding
- public key infrastructure/electronic signatures
- passwords

The Internet

The Internet—a worldwide information network linking computers, accessible to the public with the appropriate technology —can be used for electoral purposes in a variety of ways. Some of the electoral applications of the Internet include:

- in-house intranets
- email
- procurement
- publishing information for voters, candidates, the media and other clients
- voter registration
- campaign finance reporting and disclosure
- election results publishing
- electronic voting

Office automation

Personal computer-based office automation software has become an indispensable part of election management in many countries. Word processing programs have replaced typewriters; spreadsheet programs have replaced ledger books; database programs have replaced paper-based electoral rolls, inventories and staff lists; and personal organiser programs have replaced paper diaries.

Word processing and spreadsheet programs developed in the 1970s are cumbersome in comparison to the sophisticated office automation programs currently available. These programs have empowered ordinary office workers by enabling them to complete tasks in-house that were once completed off-site.

For example, desktop publishing programs allow relative novices to produce professional-quality publications, instead of using professional typesetters and printers. Database and spreadsheet programs running on high-powered personal computers allow ordinary users to input, store and use data in ways that once would only have been possible on large main-frame computers operated by programmers.

Specialised electronic/mechanical devices

In addition to standard computers and electronic voting devices, there is a wide range of specialised electronic/mechanical devices that can be used for electoral purposes:

- counting machines
- letter openers
- mail inserting machines
- label printers

- overhead projectors
- televisions/videos
- electronic whiteboards
- date stampers
- automatic numbering machines

Non-electronic Innovations

Some uses of technology for election purposes are not electronic or mechanical, but involve the innovative use of manufactured materials such as:

- plastics for ballot boxes, voting compartments and security seals
- cardboard for ballot boxes, voting compartments and polling place furniture
- tamper evident materials
- dyes and inks to prevent multiple voting

Telecommunications Technology

Telecommunications technology refers to distance communications, such as radio, telephone, television, satellite, microwave, data communication, and computer networking. In the 21st century, it is essential to the conduct of most elections.

Depending on the country, all or some of these telecommunications technologies are used by the electoral administration to transmit information: via voice in telephony and radio, documents in faxes or data including text, sounds and images, in computer networks.

Telecommunications technologies continue to evolve rapidly and are becoming increasingly affordable and reliable to communicate voice, data and even images between distant and isolated places around the world. This facilitates the organisation of elections by enabling communication of electoral officers stationed at remote locations with their respective regional and national offices.

The main components of a telecommunications system are: the transmitter, a device that originates communication; atmosphere or cables, the medium over which the transmission takes place and the receiver, the end point of the transmission.

Depending on the telecommunications infrastructure available in a country and the budget for investing in communications and equipment, electoral administration use of telecommunications can include:

- standard phone and facsimile telecommunications lines
- mobile telephones

The transmitter transforms or encodes

the data/message into a signal, which is transmitted to one or more receivers that decode it to make it understandable to the user, a person or a computer or other piece of hardware. This transmission can be bi-directional, if at the end of the transmission path there is a combination of transmitter and receiver. In the case of a "broadcast" signal the transmission goes only from one transmitter to many receivers, such as a radio or television set.

As the signal travels through the transmission medium from the transmitter to the receiver it is likely to be degraded or even modified by the interference of other signals. Most of the time, the decoding mechanism is capable of recovering the message and making it understood by the final user of the message.

Specific security issues are associated with the use of telecommunications systems. In particular, there is the possibility of undesired or unauthorized modification of the transmitted signal or message, between the transmitter and the receivers. For example, interference with telephone transmitting signals can result in conversations being heard by third parties without the knowledge of the people at both ends of the transmission path. There is also the possibility that data can be stolen or modified during its transmission by interfering with the radio frequency emissions that carry the data.

Electoral administrators need to be aware of the possibility of a security breach when data such as the results of vote counting, voter data registration or even payments to third parties are transmitted from one place to another.
Telephone and facsimile are frequently used by electoral officials. Besides personal communications, electoral authorities can use the telephone for public communication campaigns and can establish toll-free telephone numbers to handle questions from voters and/or for voting.

Mobile telephones provide a flexible alternative to standard telephones, particularly where there is no reliable infrastructure for standard telephones. They may also be a faster and more affordable way to create a voice communications network.

Mobile phones can also facilitate communications among offices that have no access to standard phones services and also between electoral offices and polling sites on Election Day.

Satellite phones and facsimiles can be used to communicate between places where no standard or mobile phone service is available. During voter registration periods and election days, this technology, if available, can solve serious problems of communications with remote areas, especially those without any access to telecommunications infrastructure.

The use of public radio by electoral administrators is probably the best method for promoting voter participation in elections and disseminating information. Radio is relatively inexpensive and has the potential to reach a wide audience, including linguistically and culturally diverse audiences as well as those who have difficulty with printed material for literacy or disability reasons.

Television is also widely used by electoral authorities to promote participation in elections and to disseminate information in many countries its reach is still restricted to a few cities and television ownership can be low. Television is also a practical and powerful medium for reaching audiences who have difficulty with printed material. However, the use of television may be expensive unless television stations consider broadcasting electoral information a public service and decide to offer substantial discounts.

Telecommunications technology also enables computers and/or groups of computers to be connected through networks, including Local Area Networks (LANs) and Wide Area Networks (WANs), making possible the communication and sharing of data. These networks employ specialized software to allow computer around the world to communicate via intranets, extranets and the Internet (World Wide Web) and transmit voice, images and data, including emails.

Networks

Most election management bodies (EMBs) need to share data stored in computers within their own administration and with outside organisations and the public. Computer networks enable two or more computers to communicate and share data and commands.

These networks, described below, may be set up by connecting computers through cables, modems, radio waves or a combination of these.

- A local area network (LAN) covers a local area, like an office or a small group of buildings.

- A metropolitan area network (MAN) usually spans a city or a large area like a university campus. A MAN typically uses wireless infrastructure or optical fibre connections to link their sites.

- A wide area network (WAN) covers a wide geographical area, involving a vast array of computers and LANs. The best example of a WAN is the Internet.

Local area network

A LAN can connect computers, workstations and other devices such as printers and scanners within a small geographic area such as an office or office building through a common communications line or wireless link. Although there are several ways to set up a LAN, typically, each computer corresponds to a node in a LAN which can execute programs and share the resources of a single computer processor or server. This means that several users can share devices as well as data located away from them. Users can also use the LAN to communicate with each other, by sending email or engaging in chat sessions.

LANs are capable of transmitting data at fast rates and may serve as few as two or three users or as many as thousands of users. However, the geographic distance of a LAN is restricted and there is a limit to the number of computers that can be attached to a single LAN.

Besides specialized hardware, a LAN requires special operating system software to allow the various devices connected to the LAN to communicate with each other and to ensure the security of the LAN resources and to control the users’ access rights to those resources.

In addition to the benefits derived from being able to share data and programs, LANs allows systems administrators to impose standards on computer hardware, software and users procedures. Users may be required to store data on the central file server rather than their local hard drives, thereby ensuring that the organizations’ data can be centrally managed and backed up and that the data is available to all authorised staff on the LAN.

Wide area networks

Several LANs can be connected to create a wide area network (WAN). WANs can allow geographically dispersed computers to communicate with each other and to share data. For example, an EMB with several different offices, each with its own LAN, can have an EMB-wide WAN, allowing data to be shared across the organisation.

WANs can be used to link computers with access to appropriate telecommunications from anywhere in the world. WANs can be connected by cables or optical fibres, or by microwave links or radio links, using ground-based or satellite transmitters. These links can be privately owned, but they are often part of the public telecommunications infrastructure.

Many WANs are organisation-specific, connecting all of an organisation’s employees to one network regardless of their physical locations. Many users do not see a distinction between their LAN and their WAN.

The Internet

The largest WAN is the Internet, which is a collection of networks linking millions of computer users around the world. It is made up of thousands of smaller commercial, academic, domestic and government networks. It carries various information and services, such as electronic mail, file sharing and the World Wide Web.

Apart from the complex physical connections that make up its infrastructure, the Internet is held together by multilateral agreements and by technical specifications or protocols that describe how to exchange data over the network. Any communications network, wired or wireless, that can carry two-way digital data can carry Internet traffic.

Millions of people worldwide have easy, instant access to a vast and diverse amount of online information through keyword-driven Internet research using search engines like Google and Yahoo.

Specific networks may use security, authentication and encryption technologies which limit the access to some or all of their information by the general public while encouraging the use of new ways of home-working, collaboration and information sharing among its authorized users.

The Internet has already proven to be a useful way for EMBs to communicate information to voters in countries where access to the Internet is widely available. Some countries are also starting to use the Internet to allow voters to cast their votes in referendums as well as national, regional and local elections.

Intranets

An intranet is a LAN or even a WAN that is set up like the Internet, but used internally in an organisation to facilitate communication and access to information restricted to its staff and authorised users.

Internet technologies are also used to provide new interfaces to corporate management information systems, such as human resources management systems, procurement and financial systems.

Several EMBs have already set up intranets containing an in-house website that is accessible only to EMB staff for administration and training purposes.

These intranets may not be connected to the Internet itself, but if they are, there is probably firewall software that acts as a gateway through which all access to the organisation’s data is filtered and can be monitored by the organisation's security department. Where external e-mail access is provided, known sources of spam and specific types of e-mail attachment can be blocked by the organisation. It should also be noted that e-mails sent and received this way can be required to be produced by the organisation in the event of legal action against it by a third party.

Extranets

Like an intranet, an extranet is a private computer network that uses Internet technology and the public telecommunication system to securely share part of its business information or operations with suppliers, vendors, partners, customers, or other businesses. Access by the general public is not authorized.

This means that an extranet requires security and privacy. These can include firewalls server management, use of digital certificates and message encryption.

The Internet

The Internet is a worldwide network of computers accessible by anyone with the necessary technology. It is used for electoral purposes in a variety of ways. The Internet evolved from a range of computer networks developed in the 1960s and 1970s by the United States Department of Defense, various universities and other institutions. By the 1990s, the Internet had evolved into a global network facilitating access to vast information and enabling electronic communication and commerce.

Some of the electoral applications of the Internet include:

- publishing information for voters, parties, candidates, media and other clients
- in-house intranets
- email
- procurement
- publishing of election results
- campaign finance reporting and disclosure
- electronic voting

The Internet consists of an immense network of computers connected by phone lines and, increasingly, by faster and more reliable “broadband” lines, including wireless media. Cabling and transmission options are quickly advancing, offering convenient, faster and affordable Internet access. Computers are connected to these lines via communication adapters, the most common example of these are modems.

Most Internet users employ two main features, the World Wide Web and electronic mail, or email.

The World Wide Web

The World Wide Web consists of a global network of computers, each one offering services or data, called websites. These websites contain interconnected “pages” of data in the form of text, still pictures, moving video and animation, and sound. Consequently, websites can provide information using a variety of delivery techniques, unlike traditional books, videos or audiotapes, which are more static and offer limited search facilities. For this reason, websites and CD-ROM programs that have the same features as websites are described as “multimedia”.

Multimedia programs contain “hyperlinks” that enable the user to navigate through the pages of data. Users can follow items of interest, rather than be locked into a sequential progression of information as in a book or video. Internet hyperlinks facilitate navigation within the same website or from one website to another, providing flexible access to information.

Simple websites are created using a programming language called hypertext mark-up language (HTML). Websites are accessed via computer programs called web browsers (Microsoft’s Internet Explorer, Mozilla’s Firefox, Apple’s Safari and others), which are widely available for little or no cost. Websites that service many hundreds or thousands of users, offering more advanced data and multimedia services are increasingly programmed in languages such as PHP, Java and others, using and following two major architectural paths. Net from Microsoft, and J2EE (Java 2nd Enterprise Edition), which is an open source software.

Most website documents are imaged and viewed by a program called Adobe Acrobat, which uses the “PDF” format. The advantage of the tools listed above (HTML, Java, Adobe Acrobat and web browsers) is that they can be run on most computing devices that are increasingly portable and wireless, expanding access to World Wide Web.

Each page in a website is identified by a uniform resource locator (URL), a unique electronic address that enables its access from web browsers via the Internet. The first words in URLs are called “domain” and they have become a standard part of the corporate identity of many businesses, and government and non-government agencies. Indeed some Internet specific businesses are known only by their domain name. The domain of the ACE Project is www.aceproject.org.

Uses of the Internet

Here are some points to keep in mind when designing and maintaining an

The Internet is both a passive and an active medium. Passive uses focus on communication of information, via still and moving images and sound, where the user simply receives information. Active uses involve two-way communication, where the users can relay information to the providers and vice versa. Active uses include email, on-line commerce and on-line information sharing, such as electronic voting or voter registration.

Many electoral authorities now have websites. In countries where significant numbers of electoral users have access to the Internet, electoral websites have become an integrated part of the service delivery strategy of electoral authorities.

Websites are an excellent way to convey large amounts of information to users. Traditional communication methods such as newspapers, brochures, radio and television are only able to carry limited amounts of electoral information. Electoral authorities can now greatly expand their information delivery capabilities by including references to their websites in their advertising. Websites can be structured to deliver as little or as much information as the user desires.

In addition to delivering information, electoral websites can also be interactive. Users can complete transactions on-line, such as applying for electoral enrolment or voting in elections. Forms can be completed on-line, such as campaign finance disclosure returns, or forms can be downloaded for printing on the user's printer and returned by mail (particularly where a user's hardcopy signature is required).

Election results can be progressively broadcast “live” on websites, as they are counted on and after election night. By the end of the 1990s, some electoral authorities were beginning to replace “physical” tally rooms with “virtual” tally rooms on their websites (for example, the Australian Electoral Commission did this with its 1999 referendum on amending the Australian Constitution).

Election results in spreadsheet or database form can also be made available on websites. Academics, journalists and other researchers can download this data for their own use.

Websites are also useful for publishing election campaign finance data, which in some jurisdictions can cover many hundreds or thousands of pages. Database technology can be used to interrogate this data on-line so as to extract particular items of interest from the vast amount of information provided.

Websites can also be developed for use inside an organisation. Internal networks, called intranets, function in much the same way as the Internet, but access is only provided to authorized users. Intranets used by electoral authorities can include internal resources, such as staff lists, user manuals, training programs, on-line electoral rolls and databases.

Website design

Website design is crucial to the operation of a website. Internet users are well known for their intolerance of websites that are slow to download or hard to understand or navigate. There are many books and Internet sites available that aim to teach good website design. As a relatively new communication medium, website design is an evolving discipline.

Electoral authorities can choose to have their websites set up and maintained by professional web designers, or they can develop and maintain their websites in-house. There are advantages and disadvantages to both choices. External designers are more likely to produce a professional result but may cost more and be slower to respond to update requests than in-house designers. On the other hand, in-house designers may not have the skills of professional designers, but they may cost less and be better able to update the site quickly and accurately.

Internet security

Internet security is a crucial issue for electoral authorities providing on-line transactions with clients, particularly on-line voting. Security is also important for email systems where sensitive information may be transmitted. Even simple websites should be protected from unauthorised changes, such as deletion or alteration of web pages or redirection of users to inappropriate off-site URLs.

Internet security is a complex field that is constantly evolving as the Internet develops and Internet "hackers" find new ways of attacking websites. Electoral authorities should consult Internet security professionals for the latest strategies available to them.

There are some general security strategies:

- Encrypt data so that only the sender and the receiver are able to decipher the information.
- Protect websites so that unauthorised users are not able to change data.
- Provide secure websites that prevent outsiders from accessing data being transmitted.

Computer Hardware and Software

Computer hardware refers to computing devices and the equipment attached to them. These may include personal computers (PCs), medium range servers, legacy mainframes (large computers that were predominant up to the 1990's), storage devices, visual presentation devices, Internet/communication equipment, imaging/printing devices, power supply management and personal identification equipment.

Computer hardware evolves very quickly offering increasing capacity and lower acquisition cost. As a general trend, tasks earlier done by mainframes and medium range servers are gradually being done by smaller but powerful PCs.

The use of computer hardware by electoral management bodies (EMBs) follows the practices of other private and public sectors. This means using generic, affordable and ever more powerful PCs and mid-range servers with standardized features. These computers are connected to institutional networks and to the Internet, which improves their affordability, controls maintenance costs and enables the development of powerful applications that assist EMBs in the fulfilment of their tasks and mandates

Personal Data Assistants (PDAs) possess powerful computing and communication capabilities—including mobile telephony—and offer great potential to EMBs. However, PDAs are still evolving and their use by EMBs was still experimental in 2006.

Computer Software refers to the instructions and commands needed to run computer hardware and to perform expected services. There are many classifications of software products, but they usually fall in two main categories: System software and Application software. System software is usually the low level software required to manage computer resources and support the execution of application programs. Application software is software that performs specific functions needed directly by the end users.

System software products include operating systems, network operating systems, data base management software, programming languages software and other software development tools. Application development products include end-user applications, office automation software and various utilities. Some software products may fall into more than one of these categories.

Operating systems control the functioning of computer hardware and enable users to perform expected actions. From a software development perspective, operating systems are very complex. The number of actions that must be flawlessly performed is very high, and the number of conditions under which these actions are performed is also high.

As a result, operating system designers must anticipate an extended variety of operational scenarios/cases as they design the software. Given this complexity, operating systems are generally created, improved and replaced at a relatively slow pace. Windows, UNIX and LINUX are probably the best known operating systems, but there are other highly specific operating systems targeted to smaller markets.

Network operating systems are a subset of operating systems. Their role is to start-up, perform and monitor communications equipment and networks. Most of these systems are proprietary but perform services defined by standards such as TCP/IP (Transmission Control Protocol/Internet Protocol), which are a suite of communications protocols used to connect computers on the Internet.
Database management software (DBMS) defines structures and tools to enable and control storage, modification, access and retrieval of data stored in a computer data base. Once exclusively proprietary, open source DBMS such as My SQL are increasingly used to create large-scale EMB applications

Programming languages software allows users to give instructions to the computer through a set of predefined scripts that define a program. Examples of programming languages are COBOL, Fortran, Pascal, C, C++, Perl, PHP, Python and Java among many others.

Software development tools include products used to assist in the main phases of development of software solutions namely design, programming and implementation.

Programming aids include Integrated Development Environments (IDE) that orchestrate the simultaneous use of program editors to write, review and edit programs; debuggers to execute and test programs that look for errors or “bugs”; and version control aids that are mandatory in multi-person software development. Almost every step in software development can be helped by special purpose programming aids—error detection, testing, operation monitoring, software usage statistics, etc.

End-user applications can be classified broadly as commercially, institutionally or custom developed. Some end user applications may include a mix of these. Commercially developed applications are bought and expected to be used with minimal or no customization. Application software developed upon request of a given institution usually requires the assistance of a third party. Samples of commercial application software are supply-chain (procurement) management, accounting software, personnel/payroll management and others that perform similar administrative services. Samples of institutionally developed software are applications unique enough that no commercial vendor has a ready made offering. Due largely to their very specific legal frameworks and national requirements, most EMBs have and use this type of software in their mandated activities.

Word Processing

Word processing software is the most widely used office automation application and most, if not all, electoral management bodies (EMBs) use it in their daily work.

By the end of the twentieth century, word processors associated with a personal computer had replaced the use of most typewriters worldwide, except in places deprived of a basic power supply infrastructure.

A word processor enables a user to create and manipulate a document, display it on a screen, store and retrieve it electronically, and print hard copies.

Unlike typewriters, word processors make it possible to correct and change the text of documents as well as exchange texts between different documents without retyping it. Illustrations such as diagrams, graphics, figures, photos and special characters can also be easily incorporated into the text, if necessary. Editing operations such as correcting typing mistakes or moving, deleting, copying and inserting text can be easily done.

These features make word processing a powerful office automation tool because it can decrease the time needed to prepare a new document or to rework an old one.

These documents can also be easily printed if the computer is connected to a printer either directly or through network connections.

Word processing features

All word processing software contains a set of basic features:

- The insert function places new text or figures anywhere in a document.
- The copy function duplicates designated sections of a document.
- The delete function erases characters, words, lines, pages or figures.
- The paste function inserts material that was removed or copied from other parts of a document.
- The format function is used to layout a document by specifying page, margin and tab size, and applying special design features such as font type and colour, bolding, italics, underlining and highlighting.
- The find and replace function searches for a specific character, word or phrase in the document and substitutes it for another one.

- The column and table function creates, manipulates and formats columns and tables.
- The mail merge function produces customized letters and documents tailored to recipients listed in a table or database.
- The file management function stores, accesses, moves and deletes computer files.
- The print function generates a hard copy of an electronically stored computer file.

Besides these basic features, most word processors are able to check spelling, insert a header/footer, footnotes and create a table of contents, indexes and cross-references.

Most word processors also offer a limited set of tools to create illustrations. These illustrations may be imported from different software and inserted into the document.

Since word processing software enables documents to be saved as computer files, several versions of a single document can be saved and accessed for comparison
For documents that need to be shared and edited by several people, there is a tracking function that enables multiples users to insert changes and comments.

The list of features offered by word processing software continues to grow as existing word processors are updated and new software becomes available.

Other considerations

Word processors combined with high-quality printers are able to produce documents that were once only produced by professional typesetters. Today, an increasing number of documents are created in-house by staff members without specific skills.

There are many uses for word processors in electoral administration. Virtually any application that involves the production of written material can benefit from use of a word processor. Most elections publications and correspondences such as books, brochures, forms, letters and newsletters can be produced in-house.

Many books, magazines and websites are available to help choose suitable word processing software. Often, word processing software is bundled with the appropriate computer hardware, either as part of a purchase agreement or as part of government or even the EMB standard for office automation tolls.

Although most software packages come with user manuals and self-paced on-screen tutorials, it is still desirable to provide training for all users. While external trainers are available in most countries, EMBs may be able to use its own skilled staff to provide in-house training.

Spreadsheets

Since its introduction at the end of the 1970s, spreadsheet software has become one of the most widely used office automation applications, replacing the manual spreadsheets and bookkeeping ledgers used by accountants for hundred of years. Spreadsheet software is able to present, display and print data in a table-like format and to perform automatic calculations on a set of figures.

Spreadsheet software is used extensively to support electoral administration activities. These include the preparation of financial records and budgets for the overall organization of elections, the planning of voting operations, and the calculation and displaying of elections results, among others. While some of these documents can also be prepared with a word processor, many users prefer the features offered by spreadsheet software.

Spreadsheet programs allow user to enter columns and rows of data. The intersection of a column and a row is called a cell. Data or formulas are entered in the cells and the formulas can perform calculations on data stored in other cells. This means that values provided by the formulas are automatically recalculated whenever there are changes to the data.

Spreadsheet software can also prepare, display and print graphs based on the rows and columns of data, making it useful for data analysis and studying trends.

Spreadsheet features

In addition to performing many types of calculations, spreadsheet software has some features similar to word processors, such as the ability to type, move, copy, delete and paste data contained in cells, groups of cells and rows or columns. Spreadsheets are saved as electronic files and can be displayed, edited and printed, provided the electronic file is not erased. This means that multiple versions of spreadsheet documents can be saved for further access as needed. Data can also be copied, moved and pasted among several spreadsheets.

Most spreadsheet software offers a basic set of features:

- The calculation function is able to add, subtract, multiply and divide elements of a formula written in a cell. There are also predefined formulas called “functions” that can perform simple or relatively complex calculations by using specific values, called arguments, in a particular order or structure. Some common functions used by spreadsheet software are “sum” to add numbers from a range of cells, “average” to calculate the average value of a set of cells, and “round” to round off a number in a designated cell.

- The chart function creates charts from the data entered in a worksheet. Once the link between a worksheet and a chart is created, the chart is automatically updated with the values entered in the respective worksheet.
- The insert function inserts cells, rows and columns anywhere in the document as well as characters and data into the cells.
- The copy function duplicates data in a cell, a set of cells, and rows and columns of a document.
- .
- The delete function can erase characters and words along with cells, group of cells, rows and columns.
- The paste function inserts material into a cell that was removed or copied from other cells.
- The format function is used to layout a document by specifying page, margin and tab size, and applying special design features such as font type and colour, bolding, italics, underlining and highlighting.
- The find and replace function searches for a specific character, word or phrase in the document and substitutes it for another one.
- The file management function stores, accesses, moves and deletes computer files.
- The print function produces a hard copy of a document prepared with spreadsheet software and electronically stored.

Besides these basic features, some spreadsheet programs are able to insert headers and footers and offer additional functions such as sorting, spell checking and tracking changes, among others.

It is also possible to insert pictures and diagrams into a spreadsheet document, although it is more complicated than doing so in a word processing document.

The list of features available in spreadsheet software continues to grow as new versions are introduced in the market.

Many books, magazines and websites are available to help choose suitable spreadsheet software. In many cases, spreadsheet software is provided or bundled with computer hardware, either as part of a purchase agreement or as part of a government or industry standard.

It is desirable to train EMB staff on how to use spreadsheet software. Most countries have external trainers, but EMBs may also be able to provide in-house training using its own skilled staff. Most software packages also come with user manuals and self-paced on-screen tutorials.

Spreadsheet programs are best used when data is being analysed in two dimensions (rows by columns). When many different kinds of variables are being analysed, or where there are many different kinds of relations between different variables, relational databases are more efficient methods of recording and analysing data.

Databases

Using a database is a more sophisticated way to store, retrieve, display and analyse data than using a spreadsheet. Database software has many potential applications for electoral purposes. For example, databases can be used for election results, party and candidate regulation, inventory control, polling place management, staffing and finance.

Before the inclusion of powerful database programs in office automation software suites in the 1990s and 2000s, database programming tended to be the exclusive domain of professional computer programmers. However, the creation of more user-friendly database programs has given the lay person the ability to develop relatively complex databases without professional information technology qualifications. Election management bodies (EMBs) now have the ability to develop databases in-house.

Data in a database is stored in tables. Each table consists of one or more records and each record may consist of one or more fields. Each field usually relates to a particular type of data. For example, a table named "Staff" may contain a record for each staff member. For each record, there may be fields for first name, last name, address, employment number, position held and so on.

Data stored in tables can be analysed, manipulated, updated, deleted, displayed and printed by applying computer instructions to the data. These instructions are usually applied by use of queries. A query is a set of computer instructions that directs the database program to perform one or more tasks. For example, a query could ask the "Staff" table to find all employees named Smith and display them alphabetically by first name.

Database forms display data on-screen in a more user-friendly and graphic format than spreadsheets and enable users to easily view and manipulate data.

Databases can also produce printed or electronic reports using data contained in its tables or data generated by its queries.

There are five main types of databases:

- flat
- network
- hierarchical
- relational
- object-oriented

Flat databases are similar to spreadsheets, with records included in simple lists. The flexibility of flat databases is limited, and they are only suitable for relatively straight forward tasks, such as mail merges.

Hierarchical databases have a treelike structure, with each level of records branching off into a set of smaller categories. This type of database is also relatively limited because sets of records only contain a single link between different levels, restricting flexibility.

Network databases contain multiple links between sets of data, allowing for greater flexibility.

Relational databases go further than network databases in allowing relations between various sets of data to be used to create complex queries. For example, the "Staff" table could be linked to a "Position" table that provides a full description of the position occupied by each staff member, and the "Position" table could be linked to a "Payroll" table that lists the salary of each staff member.

Object-oriented databases have similar attributes to relational databases, however more complex data structures called "objects" are used. Object-oriented databases are the most flexible and adaptable type of database. Most modern databases are relational or object-oriented, or a combination of both.

Database programs supplied with modern office automation software are powerful and allow relatively unskilled EMB staff to easily produce simple databases. Skilled users can develop sophisticated products. For example, an electoral authority could use database programs to:

- enter, store and use electoral roll data
- automate various parts of the election process, such as issuing and receiving postal votes
- capture and analyse election results data
- store and manipulate employee records
- automate large scale personalised mailings to clients and staff
- keep inventories
- record candidate details and facilitate the printing of ballot papers and the reporting of election donations and spending

Other technologies

In addition to standard computers and electronic voting devices, there is a wide range of specialised electronic/mechanical devices that can be used for electoral purposes. For example:

- counting machines
- letter openers
- mail sorters
- label printers
- overhead projectors
- televisions/videos
- electronic whiteboards
- date stampers
- automatic numbering machines

Counting machines

Various kinds of electronic counting machines are available for counting paper ballots. Many of these were originally designed and built to count bank notes. A variety of counting machines are available to count different sizes of ballots.

More complex counting machines can count ballots in batches (such as batches of 20, 50 or 100) as well as keep a running total of all the ballots counted for a candidate or a ballot option.

Counting machines are generally faster and more accurate than counting by hand.

Letter openers

Many kinds of electronic letter opening machines are available, from small, low volume machines to larger machines capable of handling high volumes of mail.

Electronic letter openers generally work by slicing a small strip of paper from the edge of each envelope. To avoid slicing the contents of the envelopes, it is preferable to ensure that the contents of envelopes are smaller in dimension than the envelopes.

Election management bodies (EMBs) dealing with large quantities of mail (for example from postal ballots) would benefit from the purchase electronic letter openers.

Mail inserting machines

Mail inserting machines allow users to place one or more items of mail into envelopes automatically. More complex machines can be programmed by computer to insert varying mail items into each envelope, depending on the needs of each addressee.

For example, a mail inserting machine used for postal voting could be programmed to insert a personalised letter incorporating an address label, a ballot paper for the voter's specified electorate, and a return envelope. Computer databases are used to specify the various kinds of mail received by each voter.

Mail inserting machines come in many variations, from simple desktop machines to large sophisticated computer-programmed devices. The larger machines may also incorporate laser printers, which can print personalised letters as the mail is being collated. EMBs are unlikely to have the need or the budget for the larger models and are more likely to provide large complex mailing jobs to professional mailing companies. However, for smaller mailings EMBs may find the smaller desktop machines to be useful.

Label printers

Specialized label printers are available, which can print labels directly on to envelopes or on to sticky labels.

Label printers come in a wide range of sizes and complexities, from small desktop printers to large high-volume industrial models. EMBs are unlikely to have the need or the budget for the larger models and are more to use professional mailing companies. However, for printing small runs or single labels, EMBs may find the smaller desktop machines are useful.

Sticky labels are also available in standard paper sizes for use with desktop printers. Standard office automation tools such as word processors and databases can be set up to produce mailing labels using these label sheets.

Overhead projectors

Overhead projectors improved considerably since beginning of the 1990s from the old-fashioned early transparency projectors. While transparency projectors are still available and useful, more advanced projectors can project images directly from a computer onto overhead wide screens.

Electronic computer projectors, combined with presentation software, can deliver very sophisticated presentations. Overhead projectors can project text, data, drawings, photographs, animations and video. Coupled with speakers, sound can be added to presentations.

Overhead projectors are widely used by EMBs for training, presentations and seminars. Projectors can also be used at public election events, such as declarations of candidates and ballot draws or results.

Televisions/videos

Television and video is also used by EMBs for training, presentations and seminars. Many kinds of wide screens are available to display television and video output in a large format suitable for big audiences. This can be used, for example, to train large numbers of polling officials, for example.

When connected to an appropriate computer/Internet system, television screens can be used to facilitate video conferencing. This is particularly useful for conducting meetings or training sessions with geographically dispersed participants.

Electronic whiteboards

Another presentation and training tool is the electronic whiteboard. The advantage of electronic whiteboards over traditional whiteboards is the ability to scroll through several different screens without having to erase previous screens, so that earlier screens can be revisited. It is also easy to print copies of the screens.

Date stampers

Mechanical and electronic date stampers of various complexities can be used to automatically date incoming and outgoing mail and correspondence.

Automatic numbering machines

Mechanical and electronic numbering machines of various complexities can be used to automatically place numbers on items such as forms received or the pages of a file.

Non-electronic innovations

Some uses of technology for election purposes are not electronic or mechanical. Most of these involve the innovative use of manufactured materials. For example:

- plastics for ballot boxes, voting compartments and security seals
- cardboard for ballot boxes, voting compartments and polling place furniture
- tamper evident materials
- dyes and inks to prevent multiple voting

While many of the behind-the-scenes processes in an election can be automated with electronic devices, the polling process itself is often a non-electronic affair. This is in part because of the enormous cost of providing electronics such as computers or electronic voting devices at large numbers of polling places for an infrequent, one-day-every-few-years event.

Nevertheless, innovative use of non-electronic technology can be employed at polling places.

Many old-fashioned ballot boxes are manufactured from wood or metal. These tend to be heavy, cumbersome and costly to transport and store between elections. Light-weight, disposable/recyclable ballot boxes can be manufactured from cardboard. Light-weight, collapsible, reusable ballot boxes can be manufactured from plastic.

Although cardboard and plastic ballot boxes are not tamper proof—a padlock on a cardboard ballot box would not stop an intruder with a knife, for example—these ballot boxes can be designed in a way to make it impossible for intruders to gain access without leaving evidence. This is usually achieved by sealing the box with uniquely numbered plastic seals. The numbers are recorded by polling officials in front of witnesses, and the seals are checked before the ballot box is opened at the end of the poll to ensure that the seals were not broken or substituted.

Voting screens used for privacy can be manufactured from lightweight cardboard or plastic. Unlike old fashioned wooden screens, cardboard or plastic screens are easier to transport and store and can be disposed of or recycled. It may be more cost-effective to buy new screens for each election rather than pay storage fees between elections.

Cardboard can also be used to make other temporary polling place items, such as tables, signs and queuing fences.

Other innovative materials include dyes and inks used to mark the fingers of voters to ensure that they only vote once in an election. Some inks are invisible to the naked eye, but detectable to ultra-violet light, making them difficult to remove. When invisible inks are used, each voter must have their hands checked under a ultra-violet light to be sure that their hands are not marked. After voting, at least one finger is dipped in the ink. Special inks and dyes that are visible may be used as long as they cannot be removed during polling.

Whether such inks or dyes are appropriate to a particular country's circumstances will depend on the likelihood that voters will attempt to vote more than once, and the cultural acceptance of such an invasive measure. Electoral authorities also need to be satisfied that the use of inks or dyes do not pose a health risk to voters or polling staff.

Managing Technology

Increasingly, technology is among an organisation’s most important resources. As such, it needs to be properly managed in order to meet the organisation’s objectives in an efficient way. Electoral management bodies (EMBs) can follow these steps to benefit from the use of technology:

- conduct detailed needs assessment studies to identify the required environment, regulations, procedures, and tasks
- prepare a business plan with a cost estimate and a benefits/risk analysis
- secure the financing necessary to acquire and maintain the chosen technology
- obtain adequate staff with technical expertise
- secure transportation, warehousing and distribution of equipment, if applicable
- ensure adequate testing procedures before any technology is adopted
- implement proper security procedures
- create a training plan for staff and user training
- establish proper maintenance and backup

procedures are in place

- give users access to a help desk
- provide a sufficient supply of peripherals and consumables materials, if applicable
- prepare adequate replacement plans and procedures for equipment that can become obsolet

The importance of managing even common technology is sometimes lost in the rush to adopt new technology and yet this could be essential to a successful implementation process.

There may be additional complications when managing technology for electoral administration. The level of external scrutiny of specific technologies may be high and approval by the legislature as well as other stakeholders in the electoral process may be needed.

The electoral environment is also relatively unusual in that technology might be obtained for a specific electoral event. In that case, the technology may have to perform once only on a specified day, when any system failure would spell disaster. Testing, verification and backup plans have to be thorough and reliable to make sure that the electoral event takes place without a hitch.

The importance of elections and the need for accuracy, security and transparency, management of technology dictates high standards.

The following topics cover the main issues related to managing technology in the electoral environment. Checklists can be developed to identify the main concerns of technology management that enable a successful electoral event.

- Planning and Development Strategies
- Quality Assurance
- Management Structure
- Computer Systems Administration
- Staffing, Training and Support
- Managing Obsolescence
- Evaluation and Audit

Choosing and Acquiring Technology

Choosing and acquiring technology can be a major undertaking for an election management body (EMB). Before committing to a large technology purchase, an EMB may find it most effective to adopt a structured approach to selecting and purchasing technology.

Steps include:

- establishing whether there is a need for technology
- selecting cost-effective technological solutions

- evaluating local infrastructure and any limitations it might impose
- considering sustainability issues
- acquiring the chosen technology
- following correct purchasing processes

Generally, the first part of a project's development is to establish the need for a new technology.

Technology has many benefits and many applications, and most EMBs make use of technology for various purposes to good effect. However, it is possible that personal interests and outside influence may prevail over the real need for a technology.

Once an EMB has decided to acquire new technology, the next step is to select the most cost-effective technological solutions available. Before making a commitment to its implementation, it is important to fully calculate all the likely costs and savings to determine whether the new technology is viable.

The readiness of the EMB and its clients to assimilate technology will also need to be determined.

Sustainability is another key consideration. Excluding special circumstances, a technology adopted for an upcoming election is supposed to continue to be useful in future elections.

Considerations on Technology Solutions

Need for a technology based solution

Infrastructure Considerations

Readiness to Assimilate Technology

Need for a technology based solution

Technology is not necessarily the solution to every electoral administration problem. While technology often enables administrative, financial and electoral processes to run faster, more efficiently and more effectively, it can also be costly and fail to live up to expectations.

Manual, non-technological processes may still have a place in electoral administration. Depending on the environment and available infrastructures, manual processes may be cheaper, more transparent and less likely to fail than technological ones. Particularly, where access to technology is not widely available or is unreliable it can create an unequal situation among users (particularly voters). In other cases a technological solution might not be sustainable in the long term, or legislative barriers may prevent the adoption of technology.

Electoral management bodies (EMBs) may want to assess the suitability of a proposed technology before it is adopted. This includes analysing the costs and benefits, determining the availability of skills to implement and run the technology and ascertaining the likelihood that potential users will accept the new technology.

It is essential for EMBs to consider the physical infrastructure and socio-political environment of a country before choosing a new technology, since these factors may limit the appropriateness of some technologies. A country with an intermittent power supply, for example, may not be the best location to implement a wide area computer network that requires a reliable power source. High humidity or high levels of dust or sand may also restrict the choice of technology. Furthermore, an electoral process may be disrupted if there is a deep distrust of technology by election stakeholders.

Infrastructure Considerations

Some of the infrastructures to take into consideration to ensure that the chosen technological solution performs adequately under local conditions include:

Telecommunications

Several types of telecommunications infrastructure may be relevant to the technology under consideration:

- telegraphy and telephony using fixed lines or broadcast signals to transmit voice, faxes, images and data
- radio systems, including public broadcast radio and person-to-person radio communication
- computer networks, including local area networks (LANs), wide area networks (WANs), intranets and extranets that connect various groups of computers together to share data and communicate
- the Internet—the electronic communications network that connects computer networks and organisational computer facilities around the world—that enables the sharing of information, access to e-mail and the transmission of messages, images and data
- television systems

- satellite systems

Physical environment

Computers and other technology are sensitive to the physical environment, such as temperature and humidity levels.

Power generation

Technology that is powered by electricity (this includes most electoral technology) requires a reliable power infrastructure. Even in developed countries with well established power grids, power can be cut-off without warning. In less developed countries the power supply can be erratic, intermittent or non-existent. In places where a continuous power supply is essential, backup power supplies should be an integral part of the technology system.

Maintenance facilities

The availability of maintenance facilities to service a chosen technology is another essential piece of infrastructure to consider.

If a chosen technology breaks down and maintenance services are nonexistent or poor, the technology is likely to be of no use. Maintenance facilities may need to be imported to support the technology. If this is the case, the cost-effectiveness of this option needs to be scrutinised.

Technical skills

The availability of technically skilled personnel to operate and manage a new technology is also an important factor.

If the local work force is inexperienced and insufficiently trained to support a chosen technology, EMBs may have to import personnel with the appropriated skills or train their personnel. Even if skilled workers are available locally, it may still be necessary to rely on external service providers.

Training staff in-house may be costly, time consuming and difficult to achieve in the short-term, but more sustainable in the long-term. Once the staff acquires the necessary skills, the ongoing cost of maintaining technology in-house may be lower than relying on external providers.

An EMB might need to ensure that it has the ability to maintain in-house expertise and that staff turnover does not deplete its needed skills base.

Importing skilled labour may ensure success in the short term, but may be less cost-effective and less sustainable in the long-term. An EMB will need to include these costs in the budget provisions. External providers who are only needed intermittently may be less expensive and more reliable than in-house staff and more likely to be experts in their field than in-house staff. However, external providers who are needed regularly or on a full-time basis may cost significantly more than in-house staff who perform the same functions.

If external providers are working in a competitive market, an EMB may be able to reduce costs by regularly reviewing its contracts and suppliers. On the other hand, if providers have a monopoly over their product or if an EMB is locked into an open-ended contract, costs may higher than otherwise necessary.

Readiness to Assimilate Technology

EMBs adopting a new elections technology must be sensitive to the readiness of the stakeholders to assimilate the technology. In some circumstances, people will expect more from a technology than it can realistically deliver. In other cases, people may be distrustful or suspicious of a technology, or they may be poorly equipped to adopt it.

Unrealistic expectations of a technology can result in new technology that is not capable of fulfilling its intended functions. This can happen if the technology chosen is not appropriate for its intended tasks, or if it cannot be maintained after installation due to inadequate support mechanisms.

A distrust or suspicion of technology can lead to delays in implementation or can halt a project altogether. When stakeholders are poorly equipped to adopt new technology, due, for example, to the absence of trained staff or reliable infrastructure, technology can easily fail to fulfil its promise.

To maximize the chances of success, there are strategies to reduce unrealistic expectations, suspicion and distrust.

Overcoming resistance to change

Bureaucratic opposition to innovation or change may occur when there are vested interests in retaining the current system. A common fear is that the adoption of technology will lead to job loss. This may happen and should be addressed by the EMB in negotiations with staff who may be affected.

Adopting technology often changes the nature of a workplace without necessarily reducing the workforce. The number of staff employed with manual tasks may decrease, while the number of staff needed to manage the technology may increase. In some cases, these staff members will be the same people, and no jobs will be lost. In other cases, new staff with different skills may need to be employed.

When the adoption of technology is expected to lead to significant changes in work practices, it is advisable for EMBs to modify their management strategy. The most important aspect of this is to regularly consult with all affected stakeholders, starting early in the process. Stakeholders who are fully informed about the reasons for change and the expected benefits are more likely to be supportive, particularly if they are given the opportunity to make meaningful contributions at the planning and implementation stages.

There may also be political opposition to innovation or change. Elections by their nature are politically sensitive, and it is possible that a new technology will be perceived as having a political impact and affecting voting patterns. It is important to consult with stakeholders at an early stage and to secure their agreement to change, if possible. Since major changes—such as the introduction of electronic voting—usually require legislative action, securing political support is essential.

The reluctance to adopt technology may also stem from a distrust of the new technology. This may be due to a misunderstanding or lack of knowledge about the technology. Again, the best solution is to consult with stakeholders and explain the rationale behind the technology. In cases where new technology will have significant implications for the electoral process, such as an electronic voting system , trust will often need to be earned by conducting thorough, transparent evaluations of the proposed system that are, ideally, independently verified.

When the considered technology affects the public, it is important to include them as stakeholders and to gain their trust in the new system. This may entail a large-scale communications campaign to inform the voting population of the proposed changes. Before launching such a campaign it may be useful to test proposals with focus groups or survey samples of the population.

Major changes, like the introduction of new voting methods and equipment, may be subject to public inquiries, such as a commission of inquiry or a parliamentary committee inquiry. Public inquiries are a good opportunity to gauge public reaction through public submissions and the media interest generated by the conduct of the inquiries. Effective cooperation by EMBs with public inquiries also promotes trust and understanding of proposed technologies.

The maturity of the political environment will also have an impact on the acceptance of new technology. A society in a transitional phase may have very high expectations, or conversely, an elevated distrust. It is good to be aware of these possibilities and to be prepared to work with them.

In more mature political environments with greater political stability, there may be a resistance to innovation on the basis that the current system works well. In this case, change has to be persuasively presented, and stakeholders have to be convinced that tangible benefits can be expected from adoption of new technology.

Managing high expectations

While some people may be distrustful or suspicious of technology, others may expect too much. This may be particularly true for people who have not had much exposure to technology and have an unrealistic expectation that technology will solve a specific problem. This can lead to a lack of trust in the overall electoral process.

EMB officials can lower unrealistic expectations by being transparent and effectively consulting with and informing stakeholders about the opportunities and risks of adopting new technology solutions.

Overcoming structural problems

Usually, new technology is most successful when there are sufficient human and physical resources to properly manage the technology. Staff or contractors who can correctly implement and operate the technology need to be available. If this is not possible, an adequate workforce will need to be trained.

If external contractors are expected to be used, their cost needs to be taken into account when adopting new technology. In this case, contractors may be needed not only to set up the technology, but also to operate, maintain and upgrade it.

Scanning local security environment

The security environment may also have an impact on the success of a new technology, particularly in countries that are in transition to democracy. If there is a risk that the election process may be disrupted by civil unrest or sabotage, a robust and flexible technology will need to be chosen that can function if part of the system becomes inoperable. This may involve developing strategies such as maintaining multiple backups of data at several different sites, or ensuring that networks operate even if one or more links are down. A manual back up system may work best to safeguard the system in the event of an unrecoverable system failure.

Peacekeeping missions can be difficult and complicated environments to implement a new technology due to the lack of infrastructure, and the need to accomplish a large logistic exercise in a short time. Many of the strategies described above may be necessary to achieve a satisfactory result.

Costs and Benefits of Technology

Introducing a new technology for electoral administration and voting operation purposes can increase or decrease costs. This will depend on the expenses needed to acquire and maintain the new technology compared to the expenses needed to maintain the old system.

However, there are other factors besides cost to consider. A new technology may bring benefits such as improvements in service delivery or transparency that are worth extra expenses. Ann assessment of the cost-effectiveness and potential benefits should be made before committing to a new technology.

Technology may appear to be expensive at the implementation stage, but may save money in the long-term, particularly where a low-cost technological solution can be found to replace a high-cost, low-tech application. Election management bodies (EMBs) need to weigh the costs and savings associated with introducing technology. These include the initial costs of purchasing hardware and software, the hiring of consultants to set up the new system and ongoing maintenance and management costs.

The expected life-span of the technology should be determined. A technology that can be re-used for more than one purpose or for more than one election will be more cost-effective than one that can only be used only once before it needs to be replaced.

Many technological solutions may cost significantly more than the equivalent manual processes that they replace. An EMB does not have to implement a high-cost, high-tech solution if a low-cost, low-tech alternative is acceptable.

Before purchasing a technology, an EMB needs to ensure that it has the funds to cover the initial implementation stage and the ongoing maintenance costs. This will generally involve obtaining commitments through the relevant government budgetary processes. A cost-benefit analysis will be required in most cases when seeking funds from the government.

A cost-benefit analysis of new technology could take the following form:

- state the purpose of the technology acquisition

- state why its acquisition is desirable
- describe the process that the new technology would replace
- state the possible problems or risks involved with continued use of the current process
- describe how the new technology would work
- state the benefits of the new technology
- state the possible problems or risks involved in adopting the new technology
- analyse whether the new technology will increase or decrease the transparency of the electoral process
- estimate all of the costs involved in introducing the new technology—including the relevant hardware, software and infrastructure necessary for communications, transport, staff, external contractors, ongoing maintenance and future upgrades
- estimate the costs that involved if the technology fails
- explain the costs associated with the current processes
- identify any costs that would be offset by adopting the new technology
- detail a timeline for implementing the new technology
- discuss the sustainability of the new technology, and indicate its expected life-span
- identify any external events necessary for the project to proceed, such as approval by stakeholders or enactment of legislative change

Planning and Development Strategies

The first step towards implementing a new technology is to prepare a plan that sets out goals and ways to achieve them.

The planning process begins with a needs assessment (also described as an “environmental scan”) that answers the following questions: What are you currently doing? What do you want to improve? What do your stakeholders expect of you? How do your managers and your staff feel about implementing new technology? Can new technology meet your identified needs and expectations? At the end of this assessment process you might (or you might not) conclude that new technology is what you need.

Once the decision is taken to introduce new technology or update existing technology, a detailed plan for securing stakeholder agreement, obtaining funds and implementing the chosen technology will be needed

After new technology has been purchased and installed, it will have to be developed and maintained. A development strategy is needed to ensure the effective deployment of the technology.

Source: "Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada (British Columbia's Chief Electoral Officer since 7 November 2002)

Information Technology Strategy

Ideally, the implementation of a particular item of technology should be part of an overall information technology strategy. Sometimes referred to as a strategic information systems plan, such a plan is generally a publicly documented vision of how information technology will be strategically managed in an organisation.

Some jurisdictions now require all government agencies to prepare and publish a strategic information systems plan.

An overall information technology strategy will encompass all aspects of an election management body's (EMB's) information technology needs. Mapping out these needs in general terms will serve to identify opportunities for obtaining new or upgraded technology, and will also indicate where economies can be achieved by pooling resources and using various items of technology for multiple uses.

Areas that could be covered in an overall information technology strategy include:

Management structure

- computer systems administration
- hardware acquisition
- hardware maintenance
- software acquisition
- software maintenance
- manual contingency systems
- general office automation systems (such as word processing, desktop publishing, spreadsheet and presentation software)
- specialised task-specific systems (of which there may be many, such as election specific systems like voter registration, polling place management, electronic voting and vote counting systems, as well as more generic finance and personnel systems)

Data management

- systems integration and compatibility
- system verification and testing
- server management

- stand alone systems
- quality assurance
- ensuring reliability of data
- data archiving, backup and version control
- systems maintenance

Communications management

- network administration
- cabling
- Internet

Staffing

- selection and recruitment
- training and development

User management

- user support
- help desk services

Computer supplies and consumables

Managing obsolescence

- evaluation procedures

Security

- encryption
- virus protection
- physical environment concerns
- insurance

Public assurance measures

- privacy standards
- public information policy

Communication systems

Email

Audio visual applications

Strategies for special needs groups (for example, people who need language services, hearing assistance or visual assistance)

Financial Management

- estimates and budgets
- expenditure control
- financial reporting
- audit procedures
- supply and inventory management

- procurement policies
- contract management

Warehousing and distribution control

Voter identification systems

Boundary delimitation systems

Geographic information systems

Publications

Public inquiry systems

Scanning systems

Mailing systems

Forms design

Research

Source:
"Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. Reviewed by Pedro Guarda.

Implementation Methodologies

After an election management body (EMB) has identified a need for a new or upgraded technology, the next step is to prepare a project development and implementation strategy.

Project development and implementation timeline

A project development and implementation strategy can be mapped out using a project timeline.

The project timeline ideally extends past the expected life of the technology. This enables all of the expected tasks and costs to be identified and also indicates what tasks and costs can be expected when the technology is due to be replaced or upgraded.

Here is a sample project timeline for a technology to be used at a specific electoral event:

- identify the need for new technology

- determine that the proposed technology is affordable
- establish that the proposed technology is achievable and appropriate to local needs
- prepare a business case, including an analysis of costs and benefits and examination of alternative options
- create a detailed budget
- gain approval by all relevant internal and external stakeholders
- obtain the necessary funding for the life of the project
- secure an amendment of relevant legislation, if any
- produce a detailed project management plan
- prepare detailed specifications of the desired technology
- publish a call for tenders
- evaluate tenders and select chosen tender
- *negotiate and sign a final contract
- take delivery of the prototype system
- test and evaluate the prototype system
- seek approval of the prototype by stakeholders
- receive the production version of the system
- *install and test the production version of the system
- have independent auditors verify the integrity of source codes and escrow source codes, as appropriate
- train users in the operation of the new system
- conduct a public education campaign, if appropriate

- deploy the system in the operating environment
- ensure that the back-up systems are in place, if necessary
- operate the system at the electoral event
- make certain that technical and maintenance crews are available during operation to ensure successful conduct of the event
- back up data as appropriate
- conclude electoral event
- debrief system users and evaluate the operation of system
- prepare a proposal to enhance the system, if needed for the next electoral event (and repeat any of the above steps necessary to seek approval and funding for such enhancements)
- maintain the system as appropriate
- implement any approved enhancements
- repeat the above steps for operation and evaluation of the system at the next electoral event

The main milestones in project development and implementation of new technology are:

- needs assessment
- specifications and development process
- testing process and implementation process

Needs Assessments, Business Cases, and Specifications

The first stage in a project development and implementation strategy is a needs assessment (also described as an 'environmental scan'). A needs assessment often starts with an analysis of the existing process to identify any shortcomings and areas that could be improved. What are you currently doing? What do you want to improve? What do your stakeholders expect of you? How do your management and your staff feel about implementing new technology? Can new technology meet your identified needs and expectations?

This is followed by an appraisal of the available technology and, if possible, an evaluation of similar solutions implemented by other (election management bodies) EMBs and organisations elsewhere.

At this stage, it is possible to follow several different strands of inquiry simultaneously:

- Technical advisors can determine whether a proposed technological solution is suitable for the intended purpose.
- Financial advisors can estimate the cost of the proposed technological solution and determine whether it is affordable.
- Project managers can determine whether there is support within the EMB for introducing the proposed technology.
- Senior management can consult with external stakeholders on the proposed changes, if appropriate.
- Alternative solutions can be explored to determine whether there are any better or less expensive options available which may not include technological ones.
- At the end of the needs assessment stage the EMB is expected to have a sound understanding of the need for change and a firm indication of a preferred option to meet that need. This information can be used to prepare a business case, which is the next stage in the project development and implementation strategy.

Business cases

A business case is used to persuade both internal managers and external stakeholders of the usefulness of adopting the proposed new technology. A business case needs to be logical and persuasive, showing clearly all of the costs and benefits of the proposal but it should not contain too much detail as to be counterproductive. If possible, the proposal may include an estimate of all costs through the expected lifetime of the proposed solution and not just the costs for the current financial year.

Most of the work needed to prepare a business case is supposed to be undertaken at the needs assessment stage. Business cases and needs assessments are meant to be persuasive, but they are intended for different audiences. Nevertheless, if a needs assessment succeeds in persuading the authors of the appropriateness of their proposal, it can go a long way towards providing the basis for a business case to sell the proposal to others.

A typical business case may contain the following elements:

- a clear statement of the needs
- a clear statement of the proposed option
- a clear statement of any other relevant background to the proposal
- an examination of other options, and a discussion of the reasons that make the proposed option the preferred one
- a statement of the non-monetary costs and benefits of the proposed option
- an assessment of the monetary costs and savings associated with the proposal, including a full costing of the proposal for the life of the project, plus future years
- an indication of what steps are necessary for approval of the proposal, such as approval by cabinet or passage of enabling legislation by parliament
- a statement of what stakeholder consultation has taken place and/or needs to take place, and an indication of stakeholder support or opposition expressed to date
- a project timeline
- a recommendation to proceed with the proposal

Specifications

Once a business case has been approved by the relevant authorities and funds have been secured, the next step is to select a supplier or suppliers of the necessary goods and services. Depending on the size, cost and complexity of the project, this may involve issuing a tender. Smaller projects may be progressed simply by seeking quotes from suppliers.

A key component of a request for tender or quote is the definitive set of specifications of the required technology. Specifications are generally intended for technical purposes rather than for informing non-technical managers. Consequently they tend to be technical and detailed. Good specifications will spell out clearly and without ambiguity exactly what products or services are being sought.

The content of specifications will vary widely depending on the products or services required. As a general rule of thumb, specifications may contain:

- a clear statement of the required products or services, giving all necessary detail
- a clear statement of the intended purpose of the products or services
- a clear statement of any other relevant background
- if appropriate, an indication of the expected cost of the required products or services, including a full costing of the proposal for the life of the project, including future years
- an indication of whether any steps still have to be undertaken before the project can proceed, such as approval by a government institution or passage of enabling legislation by parliament
- a project timeline
- an indication as to whether the various specified requirements are mandatory or optional
- a statement as to whether the goods or services have to conform to any recognised standards or quality controls
- a list of any testing requirements that have to be

satisfied before implementation can proceed

- a description of the required levels of security applicable to the project, if any
- a description of any documentation that may be required, such as technical manuals, users manuals or contractors' reports
- an indication of whether training is required as part of the service
- an indication of how proposals submitted by suppliers will be evaluated
- a request for a quote on how variations to the specifications may affect the cost of the project (for example, if extra work is undertaken, what extra costs will be incurred?)

The above list is by no means exhaustive, and other considerations may be applicable to a particular case.

The most important information to include in any specifications is the details of the desired product or service. If possible, it is advisable to anticipate all likely variations to a project's specifications and include them in request fro proposal (RFP) from the beginning. Cost over-runs often occur when specifications are altered after the initial specifications have been prepared and the suppliers have been chosen. Careful consideration at the specification stage may save a project from running over budget, and will maximise the chance of the project's success.

Development

The development stage is the second major step towards acquiring new technology for electoral applications. It follows the needs assessment and approval process that results in choosing a supplier and it precedes the testing and implementation stages.

The complexity of the development process will depend on the complexity of the technology being implemented. If the technology is a standard off-the-shelf product, the development stage will already have largely taken place. However, many electoral applications of technology involve more than standard products. In some cases, standard products may have to be adapted or modified to perform tasks other than those for which the products were designed. In other cases, new products may have to be designed and built to meet a specific electoral need.

The development process generally involves the election management body (EMB) working with the suppliers of the products or services to ensure that the products or services are fit for their intended purposes. This may be a short process, for standard products, or a long one, where a product has to be designed and/or manufactured especially for the EMB's purposes.

Prerequisites for project development

At the start of the development process, the following steps will likely already be in place:

- The need for the new technology has been identified.
- It has been determined that the proposed technology is affordable.
- It has been established that the proposed technology is achievable and appropriate to local needs.
- A business case has been accepted by the appropriate authorities and approval has been gained from all relevant internal and external stakeholders.
- Funding has been secured for the life of the project.
- Amendment of relevant legislation has been secured, if necessary.
- A detailed project management plan has been prepared.
- Detailed specifications of the desired technology have been prepared.
- Suppliers of the desired technology have been chosen, following an appropriate selection process and contracts have been finalised.

If the project specifications have been thorough and complete, they can be used as blueprints for development and as yardsticks against which project completion can be measured. If the specifications are sketchy or incomplete, the development stage will be more difficult.

Project development methodology

The project management plan will set out the steps necessary to develop the new technology. These steps could include:

- establish a management team with overall responsibility for the project
- appoint a technical team (which could involve internal or external staff or consultants) for technical management of the project
- determine a development timetable
- agree with suppliers on a payment schedule based on the achievement of significant milestones
- set up appropriate liaison mechanisms with the suppliers, which could be a regular meeting structure
- consult with users to determine their needs and to keep them informed of developments—this could be achieved by setting up a user group
- liaise with suppliers to ensure specifications are clear and understood
- provide suppliers with more detail and/or amend specifications as necessary as development continues
- loan EMB staff to the suppliers to work closely with them on development, if appropriate
- give feedback to suppliers on prototypes, mock-ups or draft products
- arrange with suppliers for timely delivery of products or services ready for testing, ensuring sufficient time remains for testing, evaluation and implementation before the products are due to be used in production

At the end of this process, the suppliers will have provided a product ready for testing. It may be a final or close to final version of the product, or it may be a prototype, depending on the complexity and originality of the product. In either case, the EMB must test the product to ensure that it is fit for its intended purpose.

Testing

The testing process is the third major step in the technology project development. It follows the development process and precedes the implementation stage.

As with the development process, the complexity of the testing process will depend on the complexity of the technology being implemented. If the technology is a standard off-the-shelf product, it will already have undergone considerable testing. While standard products may not be perfect, most likely their limitations will be well known.

However, many electoral applications of technology involve more than standard products. In some cases, standard products may have to be adapted or modified to perform tasks other than those for which the products were designed. In other cases, new products may have to be designed and built to meet a specific electoral need. These kinds of products will require rigorous testing for the election management body (EMB) to be satisfied that they are fit for their intended purpose.

The testing process generally involves the EMB working with the suppliers of the products or services. The process can vary greatly in length, depending on how rigorous the testing.

For most items of technology, a structured, documented testing strategy should be prepared before the technology is delivered for testing. The testing strategy ought to be designed to test that the product correctly performs all of the required functions as per the specifications.

In particular, where the technology is to be used in large quantities or in high-pressure situations involving tight deadlines or large quantities of data or users, it is wise to subject the technology to load tests to ensure that the technology will stand up to the pressure of the real event. Given the high-pressure nature of elections, this aspect of technology testing is crucial to the success of the electoral process.

The testing strategy, which is part of the overall project management plan, sets out the necessary steps to test the new technology:

- allocate responsibility for testing to appropriate technical committee

- take delivery of prototype system or production version of system, as appropriate

- assemble the system in a test environment
- apply structured tests to system, noting in writing where the system does or does not meet the specifications
- establish a panel of users to test the system in a simulation environment
- include external stakeholders in the testing process, if appropriate
- request that suppliers correct any identified problems and resubmit the system for further testing
- conduct high-load tests (after initial low-load testing indicates the product is fit for purpose), simulating as close as possible the maximum load expected under real conditions
- have independent auditors verify the integrity of source codes and escrow source codes, as appropriate
- provide the technical committee and the management committee with a report on the results of the testing
- move towards implementing the system once it has passed all tests and management has agreed to proceed,

If tests up to this stage have involved only prototypes or limited quantities of the required product, the production version of the system will need to be tested again after installation, particularly where the product is networked and/or geographically dispersed.

Once the production version has been delivered and passed testing, the implementation stage can begin.

Implementation

The implementation process is the final major step in technology project development following the testing process. Despite all the work necessary to reach this point, the this stage can be the most difficult, since it incorporates the actual use of the technology in production mode.

As with the development and testing processes, the complexity of the implementation process will depend on the complexity of the technology being implemented. If the technology is a standard off-the-shelf product, it may be relatively easy to deploy and use. Users may also be familiar with the technology, if it does not depart dramatically from technology previously in use.

However, where the technology being implemented is new, untried or a significant departure from previous practice, the implementation process will have to be managed carefully.

The implementation strategy, which should set out in the overall project management plan, will provide the steps necessary to test the new technology. An implementation strategy for a new technology system to be used at an electoral event could include the following steps:

- allocate responsibility for implementation to an appropriate technical committee and an appropriate management committee
- take delivery of the production version of the system
- assemble and deploy the system as needed
- conduct final tests of all elements of the production version of the system
- customize the system, if necessary, and test and approve any changes
- prepare the system documentation, such as technical manuals, user manuals and training materials
- recruit or appoint staff to operate the system, as necessary
- train users in the operation of the new system
- demonstrate the operation of the new system for stakeholders, if appropriate
- conduct a public education campaign, if appropriate
- enter data in the system as needed (this data could be “set-up” data, such as polling place details, as well as “live” data, such as election results)

- verify data as needed (for example, keying all data twice and comparing the two versions, or requiring a second officer to check data entered by another officer, or running computerized “logic checks” on data)
- back up system programs and data as appropriate before the electoral event
- control any update processes through careful “version control”, ensuring that all relevant equipment uses the correct hardware or software version
- conduct system maintenance according to a documented maintenance schedule, as needed
- ensure that back-up systems are in place, if necessary—these could include alternative manual systems
- guarantee alternative power supplies, if necessary
- operate the system at the electoral event
- make sure that technical and maintenance crews are available during operation to assure successful conduct of the event
- back up data as appropriate during and after the electoral event
- conclude the electoral event
- debrief system users and evaluate operation of the system
- prepare a proposal to enhance or reuse the system, if needed for the next electoral event
- maintain the system as appropriate
- implement any approved enhancements

Development and

Implementation Timeframes

New technology cannot be implemented quickly without running the risk of failure, in most cases. This is particularly true in the electoral field, where election-specific technology must work effectively the first time. With an election, there is usually only one chance to get it right.

The amount of time needed for the development and implementation of new technology will depend on the complexity of the technology being implemented. If the technology is a standard off-the-shelf product, it may be implemented relatively quickly.

However, many electoral applications of technology involve more than standard products. In some cases, standard products may have to be adapted or modified to perform tasks other than those for which the products were designed. In other cases, new products may have to be designed and built to meet a specific electoral need.

In these cases, the amount of time needed to complete a project development process should not be underestimated.

Checklists provide a good indication of the number and complexity of tasks that must be completed before electoral technology can be implemented.

The tasks required to implement a complex technological project such as a computerised voter register or an electronic voting system may take months or even a year or more to implement. In many cases, the more time available, the more likely that the project will be a success.

It is not practical to predict the average time needed to implement an electoral technology project, since this will vary with the complexity of the project and the available resources. However, some examples of real-life electoral technology projects can provide guidance.

The implementation of a particular type of electoral technology is supposed to be part of an election management body's (EMB's) overall information technology strategy, and EMB’s need to ensure that time and resources are available for the project.

Each EMB's particular electoral cycle will impact on the time available to complete projects. For EMBs with a short election cycle (two years between major elections, for example), a choice has to be made as to whether it is possible to implement new technology within that short window of opportunity, or whether it is better to plan for the next election in the cycle.

EMBs that have longer election cycles—fouror five years between major elections—have the luxury of significantly longer windows of opportunity.

It may be a mistake, however, to allow too much time to complete an electoral technology project. The rate of change in technology in the 2000s is so rapid that some items of technology only have a one-to-three year life-span. This factor is a reason to delay the actual purchase and installation of hardware and software until the last practical moment. This does not, however, mean that planning and development stages have to wait until the last moment. A project plan can commence and the early stages of the project can be completed in anticipation of more advanced technology becoming available towards the end of the project cycle.

There are essentially fourstages to the recommended project development and implementation methodology:

- needs assessments, business cases and project specifications
- development process
- testing process
- implementation process

Sufficient time needs to be allocated to each stage to ensure that the technology is implemented effectively.

The first stage, which includes preparation of a needs assessments, a business case and project specifications, can take more time than expected. External stakeholders may have to be consulted during this stage and other events often have to occur, such as government approval and the passage of legislation. As a result the EMB often has little power to speed up the process.

In particular, requests for funding may have to conform to the standard governmental budget cycle, which means there may only be one opportunity in a fiscal year to seek funds. If that window is missed, an EMB may have to wait until the next year.

One way to speed up this stage of the project is to undertake several strands of the process at the same time. For example, once the need for new technology has been established and (in-principle) approval has been gained, other elements of the project such as business cases, financial approval, stakeholder consultation, specifications and legislative or regulatory changes can be pursued concurrently. However, an EMB needs to be careful not to over extend itself—a sloppy business case, for example, could lead to refusal to finance the project.

The timing of the second stage, project development, will depend on the complexity of the project. Potential suppliers should be able to provide an indication of expected timeframes for particular projects. Again, off-the-shelf products will be developed more quickly than products that have to be specially designed, programmed or manufactured.

The EMB may have to provide staff resources to assist suppliers to enable them to meet development deadlines, particularly where products are being tailored to the EMB's particular circumstances.

The third stage, the testing process, may also take longer than expected. The amount of time needed will depend on the complexity and novelty of the project. A specially tailored product will generally take weeks or months to testi. More time will be needed for further development and testing if trials indicate that the product requires amendments or changes.

It is very important to resist the temptation to cut corners at the testing stage Thorough testing identify flaws that could otherwise prove disastrous.

Liaison with other EMBs or agencies in other fields may identify similar projects to the one under consideration, which may help to determine the amount of time needed for the various stages of the project implementation.

At the implementation phase the technology is deployed and readied for use. The list of tasks to be completed at this stage is long and varied. As effective implementation is crucial to the success of the project, sufficient time should be allowed for this process.

It should be possible at the implementation phase to conduct several activities simultaneously. For example, system deployment can occur concurrently with user training, preliminary data entry can take place during backup planning, and so on. However, some activities have to transpire before others. For example, the preparation of training documentation and staff recruitment has to happen before user training can begin.

In summary, developing and implementing new technology generally takes longer than expected, and every effort should be made to devote the maximum amount of time possible to any new technology project.

Data Conversion

The adoption of a new technology for electoral purposes may result in incremental or radical changes. In either case, there may be a need to convert data from the old system format to the new one. This conversion can consume time and resources and needs to be carefully considered when choosing and evaluating new technologies.

When switching from one office automation software to another, the issue of converting data might not be too important, because this software comes often with automatic converter programs.

However, where data is stored on out-of-date systems, particularly those no longer supported by the companies that created them, data conversion can be a serious issue. In these cases, it may be difficult if not impossible to convert the data into a format that can be read by the new software.

There are a number of strategies that can minimize the problems of data conversion:

- regularly back up data in a standard non-proprietary format, such as ASCII (American Standard Code for Information Interchange)
- consistently update software to ensure not only that it conforms to current standards but that related data can be automatically converted to the newer formats
- use standard data formats across applications
- document the data collection, storage and archive practices, so that information on the data hold by the office and its characteristics is kept.
- clearly label archived data, so that it can be identified in the future
- ensure that data is stored in a current storage medium so that they can be read at a later time. While new and more efficient data storage devices are being developed, often the old devices are no longer supported by the current technology. This is the case with many types of magnetic tapes that were once widely used to store data. As a result, several institutions can no longer access important data that was stored for future use.

- ensure that the computer operating systems are capable of sharing data with the newer operating systems, since data stored using an out-of-date operating system may be unrecoverable

- ensure the conversion of data stored in a system that is going to be replaced by a new one. This includes not only the storage medium but also the hardware and software that make it possible to manipulate the data.

- keep hardcopy records of crucial data so that if all else fails, there is a possibility to convert the data by re-keying or scanning data from hardcopy records.

Often conversion issues arise when there is a need to update systems using products from different companies. Many software products include conversion programs that convert data stored under another program into their own format, but this usually only includes the most widely used ones.

When new software is being considered, it is important to check if existing data will need to be converted into a new format and how this can be done. Even where conversion facilities exist, some functions may not be supported by the new software. As a result, some data may be lost and a great deal of work may have to be put into converting the data.

Systems Integration and Compatibility

There are a number of different technology systems that can be used for electoral purposes. Many of these systems have the capacity to share common data and common software. The power of technology can be amplified if these systems are integrated and compatible with one another.

The best way to achieve this is to include these two elements in the organisation's overall information technology strategy. This strategy can be used to ensure that compatible hardware and software is purchased throughout the organisation for the various systems in use.

Systems integration

Most electoral computer systems are dependent on data. Much of the information held by election management bodies (EMBs) is used for more than one purpose. For example, lists of electorate names are used for voter registration, ballot design, polling place management, staff assignment, candidate nominations, election results and so on.

By integrating the various systems used by EMBs, it is possible to minimise data entry and maximise data accuracy by ensuring that particular kinds of data are entered, stored and maintained in only one location. Thus a data file containing lists of electorate names can be entered and maintained by the staff responsible for redistricting and shared by all other applications that need to use that data file. The same principle can be applied to any data file in an integrated system.

There are numerous advantages to avoiding the duplication of data. It can significantly reduce staff costs by removing the effort required to enter data several times. It also reduces the risk that contradictory or out-of-date data are held by the EMB.

Another benefit of systems integration is that, for the user, the differences between the various systems may be smaller than for separate stand alone systems, and in some cases the differences might be invisible. Systems can be integrated to the point where, as far as the user is concerned, there is only one system. This can reduce training costs and increase productivity.

System integration and the sharing of data by various systems has some risks. The integration needs to be carefully planned and documented, so that changes in one system do not have unintended consequences in others.

The amount of work needed to change an integrated system tends to be greater than for stand alone systems. Integrated systems are also susceptible to widespread failure if trouble occurs in one part of the structure—another problem that does not occur in stand alone systems. However, in many cases the advantages of integrated systems outweigh the costs.

Systems compatibility

Systems compatibility is related to the issue of integration. In order to share data between systems and for users to have access to seamless systems with common interfaces, the various systems must be compatible. In this context, compatible means sharing compatible hardware, operating systems and software.

One way to ensure compatibility is to use hardware with common operating systems and capabilities, often by purchasing all hardware from one supplier, and at the same time to use integrated software suites from the one supplier. While this approach can lock an EMB into a long-term relationship with a particular set of suppliers, thereby reducing the opportunity for achieving savings by competition, it maximises the compatibility of the various components of the systems.

Another advantage of using compatible systems throughout an EMB (or throughout a wider set of government agencies if appropriate) is that it has the potential to significantly reduce maintenance and upgrade costs. Where systems are common, technical staff will need to be familiar with a smaller set of hardware and software than if a wider variety of systems were in use. Economies of scale can also result where the same hardware and software is purchased in bulk.

Training costs are also reduced if various systems are compatible. In particular, if all software in use is from the same supplier, common commands and processes will generally apply throughout, thus making it easier for users to be trained and become accustomed to them.

Compatible software is useful even where systems are not integrated. Use of compatible software ensures that various kinds of files such as word processing documents, spreadsheets, data files and email can be shared between staff in various locations without any concerns about data conversion or inability to read others' files.

An issue to keep in mind is compatibility between different versions of the same item of software. Software is regularly upgraded, many on average every two to three years. Between major upgrades, minor upgrades or “service packs” can be released, mainly intended to correct problems or bugs. It is important to manage this process, known as “version control”, to ensure that all users are equipped with the same version of the software. If different users have different versions, compatibility problems can arise, even within the same software.

Efficiencies can also be gained by choosing systems that are compatible with external agencies. Some governments have adopted whole-of-government technology standards that enable the benefits and economies of scale of using common systems to be realised across a range of agencies.

Quality Assurance

Technology is often crucial to the successful conduct of the election. Therefore election management bodies (EMBs) need to ensure that the quality of the technology they use is of the highest standard.
Some steps that can be taken to ensure quality assurance include:

- prepare and follow an overall information technology strategy
- appoint management and technical teams with

responsibility for the project
- prepare and follow a detailed project plan that is consistent with the overall information technology strategy—include expected standards and performance measures
- prepare detailed and all-inclusive specifications for the project
- work closely with suppliers during the project development phase to ensure that the products meet the specifications
- conduct a thorough, documented testing process, ensuring that all aspects of the technology are tested and that it is fit for its intended purpose—this includes load tests that simulate as close as possible the real life use of the technology
- follow a structured implementation process and ensure that all stages are carried out to the standards set out in the project plan
- after technology is ready for use, conduct further tests to be sure that the production version meets the standards set by the test product
- follow a regular maintenance and monitoring program as appropriate to ensure that the technology remains effective over time
- regularly review the technology to determine whether it has become obsolete or needs upgrading or replacing
- employ specialist technical experts and/or external auditors to provide independent advice at any of the above stages
- consult with stakeholders at appropriate stages to ensure their needs are met

Financing Technology

Elections technology can range from being relatively inexpensive to very expensive. As a result, financing technology can become a crucial part of the implementation process.

In the long-term, the use of technology is likely to reduce costs and increase the efficiency and productivity of electoral administration. In the short term, however, acquiring and implementing technology are likely to lead to significant cost increases. In particular, costs can increase substantially when new systems or hardware have to be developed and purchased and when a new system is introduced in tandem with an old one.

Securing the funds necessary to implement new technology or upgrade existing technology is an essential component of any technology implementation plan. Secure and ongoing finance must be acquired before technology acquisition can proceed beyond the planning stage.

There are several steps involved in securing the funds necessary for acquiring technology.

Affordability

Before committing to implement a new or upgraded technology, election management bodies (EMBs) must determine its affordability.

Indicative costing quotes of the proposed technology needs to be obtained to assess whether the estimated expenditure is realistic given the particular circumstances. Where several new technologies are being considered, it may be necessary to prioritise the available options and if necessary, discard those that are not affordable given the funding restraints.

How easily a quote can be obtained depends on the complexity of the technology. If the technology is a readily available off-the-shelf product, such as standard software or computer equipment, prices are usually easily obtained from local suppliers. Comparing quotes from a number of different suppliers—if possible, at least three suppliers—is a good practice.

Obtaining quotes for specialised or customised technology can be more difficult. There are a number of different strategies that can be used in this instance. For example, it may be possible to find other EMBs or organisations that use the same or a similar kind of technology to the one being considered. These other organisations may be willing to provide the cost of the systems they use.

Another method is to approach possible vendors and ask them to provide a quote based on a draft of the specifications for the proposed system. Care needs to be taken to ensure that the proposed system is described in sufficient detail to enable a quote to be relatively accurate.

A request for proposal (RFP) is a more formalised approach to seeking quotes and is not as binding as a tender process. This process involves issuing a set of specifications similar to, but not as detailed, as tender specifications and asking for cost proposals from suppliers that meet the project specifications. RFPs not only supply quotes for budgeting purposes but may also help refine the specifications for the technology being considered.

When determining whether a proposed technology is affordable, the cost of the technology over its whole life needs to be calculated. In most cases, this will include not only the purchase or lease cost but also maintenance costs, peripherals, consumables, software development, communications, upgrade costs and disposal costs.

Budgeting

After deciding that a particular technology is affordable, the next step is to prepare a detailed budget that takes account of both the immediate and the ongoing costs associated with the chosen technology.

There are four components to a technology budget: the list of goods and services to be purchased, the cost of each item, the schedule of payments, and any expected savings related to the new technology. Except in the case of items that are only to be used on one occasion and then disposed of, most items of technology will require ongoing funding for maintenance. Funds will also need to be secured for the life of the technology.

Funds acquisition

Once a detailed budget has been prepared, the next step is to acquire funds from the appropriate government or non-government source. The success of this process depends on preparing a strong business case with clearly identified benefits and a thorough budget.

Therefore a business case needs to justify the need for new technology to the funding authorities. If there are increased costs with the use of a new technology, the non-material benefits, such as increases in accuracy, speed and efficiency, need to be stressed. Other circumstances may be easier to justify, for example, when a less expensive technology replaces a costly manual process. However, it is important to ensure that all costs are properly factored in the budget.

It may be possible, in some situations, to use innovative funding mechanisms, such as joint ventures or leaseback arrangements provided there is no perception, justified or not, that the EMB is behaving unethically.
Once agreement has been obtained to provide funds, funding will need to be available in time for adequate development, testing and implementation of the new technology.

International funding

Depending on the circumstances, international funding may be available. This usually applies where external funding is an option, particularly where aid is being provided by other governments or by non-governmental organisations (NGOs). In these cases special issues may arise, such as foreign exchange issues, uncertainty of funding availability, or the potential for conflicts or impositions regarding, for example, the sourcing of suppliers.

Depreciation and amortization policies

When calculating budgets for the life of a project or a technology, depreciation and amortisation policies will impact on the calculations of costs and benefits, particularly in future years.

At the end of the life cycle of a technology item, the question arises as to whether it is more economical to use or dispose of obsolete equipment. As improvement in computer technology accelerates, this issue can emerge within a year or two of purchase. In cases where the technology continues to perform satisfactorily, notwithstanding that it is obsolete, it may be worth retaining. In other cases, it may be desirable to upgrade the technology and resell the old equipment while it retains some value.

The issue of when to upgrade obsolete equipment must be taken into account in a budget, since it will impact on the cost of the technology in the long-term.

Budgeting

After deciding that a particular technology is affordable, the next step for an electoral management body (EMB) is to prepare a detailed budget. The budget needs to take account of both the immediate and the ongoing costs associated with the chosen technology.

There are four components to a technology budget: the list of goods and services to be purchased, the cost of each item, the schedule of payments, and any expected savings associated with the new technology. Except in the case of items that are only to be used on one occasion and then disposed of, most items of technology will require ongoing funding for maintenance. Funds will also need to be secured for the life of the technology.

Budget items

Depending on the type and scope of the technology being considered, these items may appear in the budget:

- hardware (purchased or leased) —for example, computers, monitors, printers, scanners, photocopiers, fax machines, communications equipment, electronic voting devices, touch screens
- software (licensed, purchased or leased) —for example, office automation, database, finance,

personnel, proprietary, Internet, communications

- hardware upgrades
- software upgrades
- communications - for example, network charges, satellite links, cabling, radio, telecommunications
- peripherals - for example, keyboards, modems, speakers, amplifiers, disk drives, disk writers, backup storage devices, ergonomic aids, emergency power supplies
- consumables - for example, printer ink and toner, paper, disks
- support for example, repair technicians
- maintenance - for example, technicians
- salary - for example, payment of staff who will be partly or wholly dedicated to working with the new technology
- consultants - for example, project management consultants, technical consultants or independent auditors
- transport - for example, transport from place of purchase to place of storage and to place of use
- energy - for example, electricity to operate the technology and associated lighting and air conditioning, power generators for emergency use or for use where local power supplies are unreliable
- storage - for example, storage during and between use
- training - for example, training full time and part-time staff to use the new technology
- public information - for example, conducting a public education campaign on the use of a new electronic voting system

- documentation - for example, system specifications, technical maintenance manuals, user manuals, training manuals

- printing - for example, documents designed to be used with the technology, such as machine readable ballots or forms

- back-up systems - for example, alternative systems such as manual systems to fall back on if technology fails, as well as systems for backing up and storing data in the event of system failure

- disposal costs - for example, costs associated with disposing of or selling obsolete technology

- depreciation and amortisation estimates - for example computer equipment expected to last three years has a cost that can be written off in a three years period which is equivalent to a depreciation of environ 33% par an.

Estimating costs

Once all the possible items of expenditure have been identified, costs, estimated for the expected life of the equipment or project, need to be assigned to each item.

Project timeline

In most cases, not all new technology costs need to be paid up front. After the initial purchase and set-up costs, usually there are ongoing maintenance and development costs over the life of the project. The long-term budget can be calculated following a timeline with project milestones payment schedules.

Where the project involves a testing and/or evaluation stage, it is desirable to make progressive payments dependent on achieving the set milestones. If there is a provision to halt a project in the event that the system fails to pass testing, the payment schedule has to be structured so as to minimise the cost to the election management body.

Final payment to suppliers is supposed to be delayed until after the successful completion of the project. This ensures that suppliers commit to the completion of the project. Penalty clauses can also be inserted in the delivery contract, to be invoked if crucial milestones are not met.

The project timeline is expected to extend up to and ideally past the expected life of the technology. This enables all of the possible costs to be identified and also to recognize future costs involved in replacing or upgrading the technology.

This timeline can be used to identify points in the project schedule where it would be appropriate to make payments for system implementation and maintenance.

Possible savings

As good practice, the budget for a new technology identifies any offset savings that can be achieved in the course of the project. For example, costs may be offset by the savings achieved by discontinuing a manual process that is being replaced with a technological solution. In some cases, the cost of the new system may be less than the old system, leading to a net saving. This is the easiest kind of new system to get funding for.

It is probable that, in the short-term, a new system incurs greater costs than the old system. This is particularly true when the old and new systems are run in parallel before converting fully to the new system. In addition, there are often significant onetime set-up costs for a new system. It is particularly important to calculate the estimated cost of the project over its whole life, as well as the projected savings, when it is more likely that net savings may be achieved in the long-term.

Funds Acquisition

Once a detailed budget has been prepared, the next step is to acquire funds from the appropriate government or non-government source. The success of this process depends on preparing a strong business case and a thorough budget, which are more likely to persuade the funding entities to provide the necessary cash.

The business case needs to clearly set out the costs and benefits of introducing the technology. When there are increased costs, the non-material benefits of the new technology such as increased accuracy, ease of use and efficiency need to be stressed. In other cases, particularly where technological applications replace costly manual processes, thereby substantially reducing expected costs, care needs to be taken to factor all costs into the budget.

It may help to justify a new proposal if the election management body (EMB) is able to identify similar applications successfully in use in other jurisdictions. Pointing to the implementation of similar systems elsewhere serves both to clarify costs and to prove the feasibility of the proposal.

It may be possible in some situations to use innovative funding mechanisms, such as joint ventures or leaseback arrangements, but these mechanisms cannot compromise an EMBs integrity either as a purchaser of goods and services or as an electoral authority.

Once there is an agreement to provide funds, it is important that funding be available to adequately develop, test and implement the new technology. A common, and often disastrous, scenario can occur when funding is provided late in the electoral cycle and there is insufficient time to do the above. The amount of time required for introducing new technology needs to be carefully estimated.

It is useful to learn how long it has taken other EMBs to implement a similar system elsewhere. In general, plenty of time needs to be available, since the implementation of new technology often takes longer than expected.

In some countries EMBs may have the opportunity to seek funding from sources outside normal government channels, such as from other governments or by non-governmental organisations (NGOs). In some cases, the acquisition of new technology may only be possible with external assistance. However, care must be taken to avoid compromising the electoral process.

The certainty and timeliness of funding for new technology is crucial. Before committing to new technology, funding for the life of the project needs to be guaranteed, otherwise there is a serious risk that the technology will not be implemented successfully. Similarly, funding has to be available early enough in the election cycle to ensure that the technology can be selected, supplied and tested before an electoral event.

If external funding cannot provide these guarantees, EMBs run a significant risk in using them If the EMB decides that the risks are worth taking, manual back-up processes will be needed to protect against a technology failure that could jeopardise the overall electoral process.

In some cases, external funding may, require that a particular supplier, product or supply source be used. These arrangements should not compromise the EMB integrity either as a purchaser of goods and services or as an electoral authority. In addition these conditions are not supposed to restrict the EMBs ability to service, maintain and upgrade any technology adopted.

If there are funding through foreign currencies, there is a need to take in account that exchange rates fluctuate with a possible impact on the funding value of external assistance. Sufficient funds may need to be available regardless of currency fluctuations.

Depreciation and Amortization Policies

When formulating a budget for the life of a project or a technology, depreciation and amortisation policies have an impact on calculating costs and benefits, particularly in future years.

Depreciation

How depreciation is calculated and taken into account depends on the locally applicable finance procedures. Where accrual accounting methods are used, depreciation is a significant factor that can heavily influence the bottom line of a project.

Unfortunately, items of technology, particularly computers, depreciate quickly. The rate of change in the computer industry is such that most computer items are obsolete within months of being purchased. Thus in many cases the value of computer equipment can depreciate so rapidly that it can be written off as worthless within two to four years.

Consequently, depreciation needs to be factored into the budget strategy in accordance with local regulations or conventions. Replacement costs of obsolete technology as well as possible gains from reselling the old equipment while it retains some value are factors that also need to be included.

Amortisation

At the end of the life cycle of an item of technology, the issue arises as to whether it is more economical to use or dispose of obsolete equipment. As improvement in computer technology accelerates, this issue can occur within a year or two of purchase.

On the other hand, if the life of a piece of technology can be extended so that it can be used over several electoral events or if the technology continues to perform satisfactorily notwithstanding that it is obsolete, it may be worth retaining. Then, the cost of that technology can be amortised over a longer period and the long-term cost of implementing technology is reduced accordingly.

This approach necessitates a deliberate decision to reuse technology even where it may, in industry terms, be obsolete. Provided that the technology continues to perform its intended service to an acceptable standard, this is generally sound practice.

In addition to avoiding the cost of upgrading to new technology, reusing existing technology has the advantage of familiarity, and avoids the pitfalls of implementing new, possibly untested, technology.

When deciding whether to reuse technology and amortise it over two or more electoral events, the cost of maintaining and, if necessary, upgrading or enhancing the technology has to be weighed against the cost of replacing it. The most economic course will depend on the particular type of technology being considered and the timeframes involved.

Disposal of obsolete equipment

The issue of when to upgrade obsolete equipment has to be taken into account when budgeting, as it impacts on the likely long-term cost of the technology.

Once a decision has been taken to dispose of obsolete equipment, it may be possible to achieve some return on the investment made on that equipment by selling it. Technology that may be obsolete in one jurisdiction or industry may be still an improvement on technology in use elsewhere. While any returns to be gained are unlikely to be a significant offset on the original purchase price, there may still be value in selling obsolete equipment rather than simply destroying it or giving it away.

Governments often have agencies that specialise in disposing of obsolete equipment on a whole-of-government basis. Some governments distribute obsolete equipment to other jurisdictions as a form of aid. Other agencies under the same government umbrella may be happy to accept obsolete equipment. For example, schools may be interested in receiving out-of-date personal computers for student use.

If these options are not available or feasible, it may be possible to sell obsolete equipment by tender or auction, or simply by setting a reasonable market price on the equipment and advertising it for sale.

Management Structure

A crucial element of implementing new technology is the appointment of a responsible management structure for the project.

The type of management structure adopted for any particular project will depend on the size of the organisation and the complexity of the project. However, there are some general principles.

A major technology project management structure should include or report directly to the chief executive of the election management body (EMB). This is a reflection of the importance of technology in electoral administration. Technology has become so crucial to the successful conduct of elections that senior management should be heavily involved in its implementation.

An EMB's technology management structure can be established under the EMB's overall information technology strategy. This will ensure that there is a consistent approach across the EMB to managing technology and that appropriate managers are aware of the overall context in which a particular project sits.

A typical EMB technology management structure might include:

- a high-level policy committee chaired by the chief executive (or reporting directly to the chief executive) and including appropriate senior managers, responsible for setting overall policy, receiving reports from lower-level committees and giving approval to projects

- a medium-level committee for each major project or set of projects, chaired by the responsible senior manager (a member of the high-level committee) and including a mix of managers and technical officers from all areas with a stake in the project, responsible for overseeing the project, reporting to the high-level committee, receiving reports from the lower-level technical committee and giving approval to more detailed aspects of the project.

- a lower-level technical committee for each project, chaired by a member of the medium-level committee and including a mix of project and technical officers with direct involvement in the project, responsible for day-to-day oversight of the technical operation of the project and for reporting to the medium-level committee

The main purposes of a technology management structure are to set the overall information technology strategy, and to approve and monitor the various stages of project development and implementation. Higher level committees concern themselves with issues of general policy and strategic direction, medium level committees ensure that projects are being conducted according to the specified project strategy, and lower-level technical committees make sure that all the technical details are covered.

In particular, technology management committees ensure that timelines are followed and standards are met. Projects that run late, skip crucial tests or cut corners on standards are recipes for disaster in the electoral field. It is management's responsibility to set realistic timelines and standards in the first place. Management is also supposed to be responsible for contingency planning in case problems arise.

It is important that responsibilities are clearly defined, so that officers in charge are able to proceed with certainty and that all aspects of a project are covered. Areas of responsibility can be outlined in the project development and implementation plan.

Senior managers involved in technology management do not have to possess technology skills or knowledge, but these skills are a distinct advantage. As electoral operations become more and more dependent on technology, so will management policies and decisions increasingly come to involve technological issues. Managers without direct technology skills or knowledge will have to rely on technical advisors. To avoid complete dependence on others or making poorly informed decisions, managers will benefit from gaining technological skills of their own.

The number of senior managers without technical expertise is likely to decrease over time. As technology becomes more common in EMBs and other agencies, and as a wider range of staff become more dependent on technology, staff being recruited to senior management will be more likely to have a background in technology. This should serve to improve the management of technology in the future.

Computer Systems Administration

As Election Management Bodies (EMB) need to use several computer systems, they also often need dedicated administration services. Some of the best practices recommendations for managing computers include:

- Identification of the services that need to be automated;
- Ensuring that information technology (IT) has the support of all stakeholders and users, and that they understand the role of IT in getting the work done;
- Estimation of total costs including maintenance and specific software development contracts;
- Preparation of a complete inventory of computer equipment and peripherals;

- Setting of standards for computer hardware and software;
- Preparing clear documentation on all procedures needed to be followed in a regular basis to run the computer systems and to maintain the computers and peripherals;
- Monitoring compliance with set information technology policies;
- Preparing user manuals and documentation to support the computer systems, so that a new staff that needs to use the system can get to speed in a short time;
- Planning for computer system replacements;
- Assessing staff expertise needed to develop, implement, run and maintain the computer systems;
- Organizing a programme of ongoing training to maintain staff up to date;
- Organizing training for users as needed;
- Assessing computer system's security risks, installing firewalls and antivirus software and ensuring that security software is regularly updated;
- Developing security procedures including control of access to the systems, backup procedures and disaster recovery plans.

This said, depending on the size and budget of the EMB it can be more convenient and cheaper to outsource some of these tasks to private service companies, so that the EMB can afford the service of highly specialized experts without incurring the full cost of a permanent in house expert.

Depending on the computer platform used, there are specialized software that can be used to monitor and manage an election management body's (EMB's) computer systems. This software can perform diagnostics, analyse and report on system performance and system availability and can identify whether there are any problems that need to be addressed. As demands on computer systems increase, monitoring of system performance becomes more important, as such monitoring may identify the need to upgrade or modify system capability to meet the greater demand.

If the EMB decides to outsource management of its computer systems, relations with vendors need to be set in a carefully drafted contract and its implementation regularly monitored to decrease the risks involved with relying on a third party for technology services.

Other Considerations

Computer systems are complex, and the number of different tasks involved in developing and implementing them make computer systems administration an important element of managing technology.

Depending on the EMB size, it is advisable to establish an EMB's computer systems administration and an overall information technology strategy. This is needed to ensure that there is a consistent approach across the EMB and that administrators are aware of the overall context in which a particular computer system sits.

Ideally hardware is purchased in accordance with the organisation's overall information technology strategy. Hardware sourced from common manufacturers or suppliers is more likely to be compatible with each other than if a range of suppliers or manufacturers are used.

Asset registers can be used to keep track of hardware. Bar codes placed on hardware assets and read with bar code readers are a useful method of conducting checks on assets.

Covering all these items of hardware in a documented maintenance program and scheduling routine upkeep and inspection by trained technicians can be an effective means of ensuring their proper working order.

Server management is particularly important. As networked systems rely on the smooth operation of their servers, building reliable server systems will likely be a key priority. Server systems generally include a range of backup methods to ensure that network down time is minimized or eliminated and that data is regularly backed up. These methods can include using batteries of servers (or 'server farms') with data mirrored on various hard drives and computers, and alternative cabling routes from workstations to servers.

All computer technology relies on hardware. As a result, hardware management is a significant part of technology implementation. Typical hardware can include:

- **Personal computers (networked or stand alone;**
- **Network servers;**
- **Backup storage devices;**
- **Printers;**
- **Photocopiers;**
- **Computer peripherals;**
- **Voting machines;**
- **Scanners;**
- **Communications equipment**

Tele Communications

Management

Communications management is very important where systems are networked and/or work locations are geographically dispersed. Communications can refer to any system for distributing sound, images or data. In the electoral context it usually refers to any communication sent by cable or transmitted by radio or microwave.

Network administration is especially crucial to the smooth operation of a networked computer system, particularly where data is shared on servers. If the network fails, this can stop an organisation from functioning effectively.

Network administration is a specialised function that should be handled by trained technicians. Consult appropriate network specialists for advice on your particular needs.

Database Management

Database management is another important element of computer systems administration. Databases have many applications for electoral purposes, and the potential size and complexity of these databases require careful management to maximise their potential.

Effective databases will be carefully designed and documented. Common standards such as field names and field structures need to be established and adhered to.

Ideally, an EMB's databases will be integrated across the range of applications used by the EMB so that common data is shared across applications. This will ensure that data duplication is minimised, and data is kept as accurate as possible.

A database management structure is often an effective means to approve and coordinate database design that ensures standards are kept and data is not unnecessarily duplicated.

Help Desk

An important element in any computer systems administration is the help desk facility. The help desk has at least a twofold purpose: to resolve any problems users have with the system, and to assist them to use the system more effectively. The help desk may also be responsible for providing users with access to systems by allocating login rights and passwords.

In a small EMB, the help desk may be one officer. In a large EMB, a help desk may need many staff. In some cases there may be several help desk teams, dedicated to different functions or different regional offices. The help desk function may be staffed internally, or may be outsourced to contractors. Help desks may also be shared with other agencies, particularly where whole-of-government computer systems are in place.

Help desks are generally most effective when they are staffed by officers with the skills necessary to provide help quickly, or who are able to seek help from appropriate technical staff as needed. In some cases, help can be provided immediately. In others, calls for help may have to be logged and dealt with when appropriate staff are available.

Where calls for help have to be prioritised, having a formal structure in place will enable help desk staff to decide which calls to deal with next. This formal structure will often be most effective if it is negotiated with and agreed to by users, so that they know what sort of priority to assign to calls for help and what level of help can be expected.

It is often useful for calls for help to be logged by the help desk and records kept of types and numbers of requests, and of the time taken to provide the assistance. This will help to identify problem areas that might need fixing by training or improving hardware or procedures.

System Library and Distribution

Where software is loaded onto a number of computers in an organisation, it is very desirable that the same software version is used on each. Use of a common version ensures that various kinds of files such as word processing documents, spreadsheets, data files and email can be shared between staff in various locations without any concerns about data conversion or inability to read others' files.

The way to achieve this commonality within an organisation, particularly a large one, is to establish a system library of software and control the distribution of that software through a documented process.

This process is aimed in particular at keeping track of different versions of the same item of software. Software is regularly upgraded, on average every 2-3 years. Between major upgrades, minor upgrades or `service packs` can be released, mainly intended to correct problems or bugs. It is important to manage this process, known as `version control`, to ensure that all users are equipped with the same version of the software. If different users have different versions this can lead to compatibility problems, as even within the same item of software files created in one version may not be compatible with another.

The most effective way to manage version control is to deny users the right to upgrade software or install new software themselves. Software upgrades must then be carried out at the instructions of the systems administrators in a controlled manner according to the documented technology strategy plan.

This then raises the issue of when to update software to a new version.

User Management

Users have to be managed by their system administrators. Some of the user management issues to be considered include:

- Providing users with login identities and passwords
- Managing user access rights (ensuring users are only able to access data they are entitled to see, by for example creating different file directories with varying access rights)
- Allocating disk space to users and ensuring users do not exceed their entitlements
- Ensuring users follow standards of system requirements (such as file name and file structure) and etiquette (such as acceptable language and content)

Computer Supplies and Consumables

Expenditure on computer systems does not stop with the initial purchase of the hardware and software. Various computer supplies and consumables are needed to keep a computer system operating. These include:

- paper for printers, photocopiers and fax machines
- ink and toner for printers, photocopiers and fax machines
- lubrication oil for various machines with moving parts
- spare replacement parts for various items
- storage disks of various kinds, such as floppy disks, tapes and CDs
- cables of various kinds
- cleaning materials
- tools for maintenance purposes

Maintenance

Computer systems do not look after themselves - they have to be maintained. Computer systems maintenance can be divided into three broad categories:

- Hardware maintenance
- Systems maintenance
- Maintaining information

Hardware Maintenance

The organisation's overall information technology strategy could document a hardware maintenance schedule. Each item of hardware will likely require routine maintenance. The manufacturers or suppliers of hardware generally provide instructions on the maintenance needs of each item of hardware.

Responsibility for routine maintenance can be set out in the information technology management structure. It is preferable (and in many cases essential) that maintenance be carried out by qualified technicians. This will usually necessitate contracting external assistance.

In some cases regular maintenance can be included in the purchase or lease arrangements associated with the supply of hardware. This practice is often very desirable as it ensures that maintenance is included in the initial budget for the hardware and avoids the risk that funds may not be available for maintenance at a later date.

Maintenance may also be necessary when hardware breaks down or performs below standard. Response arrangements to such non-routine maintenance can also be included in the organisation's overall information technology strategy. Ongoing arrangements with maintenance and repair technicians will allow problems to be dealt with quickly. Prioritizing needs in advance will allow requests for maintenance to be dealt with as quickly as needed, at a pre-set price.

For example, a schedule could be drawn up showing crucial items that must be fixed within an hour of breaking down, other important but less crucial items that must be fixed within 24 hours, and less important items that must be fixed within a week. The cost of these varying levels of service will generally be higher when a faster response is required.

Systems Maintenance

Computer software systems require constant maintenance. Some of the tasks required include:

- Establishing logical file structures and ensuring users are aware of how they are to be used
- Controlling user access to systems
- Obtaining software licences and ensuring that licence conditions are not breached

- Maintaining consistency across various systems to ensure they are compatible and work is not duplicated
- Maintaining network servers and responding to problems as they arise
- Monitoring available system resources, such as disk storage space and system speeds, to ensure that disks do not become over full or that system performance is unacceptable
- Responding to requests for assistance from users
- Managing interfaces with other systems, such as internet, email and intranets
- Identifying and repairing bugs or faults in software
- Upgrading software as necessary
- Providing, monitoring and upgrading security measures such as virus protection, encryption, firewalls and hacker prevention

Maintaining Information

Computerised information, particularly data and computer programs, must also be maintained to ensure that problems do not arise and that data is available for users when they need it.

Data backup

It is generally accepted that data should be regularly backed up at least once each working day, or even more often if crucial data is being collected, such as during an electoral event. Data can be backed up on a wide variety of formats, including removable disks of various kinds, multiple hard disks, or magnetic tapes.

The organisation's overall information technology strategy could document a formal backup regime. Ideally, data backup can be automated to ensure that human error does not cause problems. However, regular checks of automated backups can also be undertaken to ensure that computer error does not also cause problems.

Live data can also be backed up as it is created, by use of mirrored hard disks, which could be located on the same server or on separate servers. Using mirrored disks, the same data is simultaneously stored on two or more disks. This means that, if one disk fails, data can be restored from the other. It is preferable to use separate servers rather than the same server for mirrored disks, as a second server can be used if the first server fails completely.

Software programs, both commercial programs and those developed in-house, can also be backed-up so they are available to reload if the production versions of the programs are lost or corrupted. Most programs come loaded on disks (although increasingly programs can be downloaded from the internet, in which case backup copies should be stored locally as there is no guarantee that the same programs will be available in future). Program disks can be stored in a data library and be managed by a responsible officer or staff unit. If needed, program disks can then be easily found and used to correct problems.

Care should be taken, when backing up program data, that software licences are not breached. Most licences include permission to keep backup copies of software.

Data security measures

Another aspect of maintaining data is keeping it secure. Computer systems can be protected by security systems to ensure that only authorised users have access to them.

Staffing, Training and Support

Technology equipment might be stand alone but it still needs people to start its functioning and to operate it. Therefore, election management bodies (EMBs) need to employ staff to look after their technology and to use the technology.

All users of electoral technology need training. This may include permanent staff, casual staff, consultants, contractors, voters, candidates, political parties or the media. The level of training required differs with the complexity of the technology as well as with the kind of user interaction.

Even after a user has been trained, there is a need for ongoing support since there may be occasions where a user requires further assistance.

Staffing

One of the technology staffing decisions facing an EMB is whether to use internal staff or external staff, such as contractors or outsourced suppliers. There are advantages and disadvantages to either course, and there might be a need to use a mix of both.

Where there is a need for full-time assistance to fulfil a technology related function, depending on locally applicable regulations, it is probably more cost-effective in the long-term to employ permanent staff. Besides the fact that external contractors tend to have a higher per-hour cost than permanent staff to compensate for lack of tenure and contract overheads, the acquired experience, institutional memory and knowledge is more easily lost.

However, where the need for technology related staff is intermittent, particularly during the implementation and training phase of technology use, it may be more cost-effective to use external contracted staff. Use of external staff for purposes with a limited life span avoids the need to find other employment for those staff when the project ends, or to pay severance.

Another advantage to using external staff, particularly for highly specialised functions, is that they are more likely to have the necessary expertise than in-house staff. This is most relevant when the technology under consideration is new to the EMB, and internal staff is unlikely to know how to deal with it. However, even with ongoing systems, external staff with an exposure to a wide range of clients and access to specialised training may be more effective than internal staff for specific work.

Conversely, an advantage of using internal staff, particularly for ongoing use of technology, is that internal staff is more likely to have a thorough understanding of the EMB's specialised systems and needs than external consultants would have. This is especially so where an EMB uses customised systems that are not in general use elsewhere.

When internal staff is used there is a risk of relying on a small number of individuals with the relevant knowledge. This can be dangerous, as all staff members move on eventually, by choice, accident or design. EMBs can take steps to ensure that the departure of key individuals do not place the operation of their technology at risk by requiring that they document their knowledge systematically so that others can operate the systems in their absence.

Another solution is to ensure that a range of staff, internal or external, are able to operate each system, so that individuals do not have a monopoly of knowledge about a system.
Since there are pros and cons to using either internal or external staff, most EMBs tend to employ a mix.

In summary, internal staff is best used on ongoing functions when there is a need to preserve institutional memory while external staff are best used for short-term tasks such as implementation and training, but they are also useful for specialised tasks requiring technical qualifications or wide experience.

An EMB might also need to employ a range of staff whose main purpose may not be to implement or operate technology, but who nevertheless may use technology every day in their occupation. Virtually all clerical and policy staff use technology on a daily basis although they are not technology specialists. In these cases, the decision to use internal or external staff depends on their main function, rather than on their technological skills. Nevertheless, as technology use becomes more prevalent, the technology skills of such staff are likely to become more relevant to their selection and ongoing employment.

Training

As mentioned above, users of technology may need to be trained. The level of training required depends on the complexity of the technology and the degree of interaction the user has with it. Training levels can range from obtaining university degrees and extensive hands-on experience to completing intensive course work or day-long courses.

Ideally, for the general user, technology is designed to be user-friendly and to require a minimal amount of training. This is particularly important where the technology is expected to be used by large numbers of people and for a short time. For example, an electronic voting system should be simple enough for any voter to use without the need for any external training. Similarly, any technology operated by large numbers of casual polling staff should be easy to use with minimal training.

Training casual staff

The training needs of casual staff such as polling officials are very different from the needs of permanent staff. Technology training has to be tailored to the limited tasks they perform, which can mean delivering training in a short, easily-digested form and recognizing that it may not be practical or cost-effective to deliver intensive, lengthy training. In this case, it is advisable to choose technology that is simple to use and requires little supervision so that minimal training will be needed.

Often technology training for casual staff is designed as a module in their overall training. If appropriate and possible, training materials, static or interactive, could also be delivered using software from a CD or over the Internet.

Training permanent “non-technical” staff

The majority of full-time or long-term electoral officials, those who perform clerical, administrative, operational, and supervisory and policy work often use technology such as word processors, spreadsheets and other office automation software tools in their daily work. In this case, technology is a tool to complete a task and some sort of formal training can help significantly to improve productivity and to extend the range of tasks that can be undertaken by “non-technical” staff.

In many countries, training companies provide training in most popular software applications. This is generally conducted in computer labs where trainees are each allocated a computer on which they follow structured hands-on programs, with a trainer leading the session. These training courses may typically run for a half day, a whole day or several days on a particular topic, depending on its complexity. Courses are usually provided at beginner, intermediate and advanced levels to cater to the ability and knowledge of the trainees.

Computer training course companies usually supply a manual and sometimes sample computer files on disk for the trainees to take with them after the course, so that the knowledge gained in the course can be reinforced and revisited by the trainee afterwards.

Another way of accessing training in how to use office automation software, particularly where face-to-face training is not readily available or practicable, is through self-learning training techniques, such as written manuals, videos, software training packages and Internet training packages.

Where large numbers of staff need to be trained in a particular technology, it may be cost-effective to employ one or more trainers to come on site and conduct the training in the workplace, using real-life systems and examples. This can be preferable to more generic training, as it can be tailored to the particular needs of the workplace, making the training more useful and relevant.

Modern office automation software often comes with built-in “help” functions and with intuitive interfaces such as buttons, menus and help wizards that enable users to operate the various systems with little formal training. In a sense, the training to use these systems is built into the systems themselves. Many staff, particularly those who are performing relatively straight-forward tasks, are able to use these systems with little or no formal training.

One way in which modern software assists this process is through the use of common standards and conventions across different programs, so that, once a process (such as the cut and paste function, for example) is learned in one application, the same process can be used across a range of applications without the need for further training. This feature is an aspect to be considered when software is being purchased—software that uses common standards across a range of applications is generally preferable to software that does not use consistent common standards.

However, while many users can operate their office software to an acceptable level of productivity with little or no formal training, there are many features of modern software applications that are not readily apparent without some training. For example, mail merges can save a great deal of effort if used effectively. To make the most of mail merge programs, it helps to understand how to link the documents to a source data such as relational databases and how to use variable fields in the merge document. Formal training can help explain the intricacies of these and similar processes, leading to increased productivity with reduced effort.

Another important aspect of technology training is that it should be an ongoing process, rather than a “set and forget” approach. Particularly because software is regularly upgraded with new capabilities, it is important to ensure that staff regularly refresh and update their skills through training. One way to achieve this is to include technology training in each staff member's training and development plan, with a commitment from the staff member and management that technology training will be regularly refreshed.

Training technical staff

Technical staff, including permanent staff and external contractors, need more intensive training to enable them to perform effectively. This may take the form of university or technical college qualifications, or specialised training for technicians.

Some companies provide accredited training courses to a recognised standard. These qualifications can be used as a guide as to the level of technical skill obtained by potential staff, and can be used by employers as a means of determining the suitability of applicants for technology jobs.

As with non-technical staff, technical staff should also keep their skills up-to-date by regularly undertaking further training to refresh their knowledge.

Since all training targets adults, it is worth considering that the methodologies have to be adapted to them with an emphasis on methodologies using participative techniques that have been found to be more effective.

Validating training

In order to ensure that time, effort and money invested in training is worthwhile, training should be validated. That is, any training program should be evaluated to ensure that it is meeting the identified needs and that it succeeds in raising productivity and delivers effective outcomes.

Care needs to be taken that technology training is appropriate to the needs of the trainee and the election management body as a whole and that it is relevant to the tasks to be undertaken by the trainee in his or her work. Since there might be a great variety of training programmes available it is important to choose those that can provide real benefits in the workplace.

Training can be validated a number of ways. One of the most important ways is to use performance measures to gauge the success of the process for which the training is being used. For example, measures of the success of training voters using an electronic voting system can include error rates, number of complaints from voters and number of requests for additional assistance; performance measures for in-house staff can include accuracy of voting results and speed with which election results are finalised.

Training should also be evaluated by the trainees. At the end of any formal training session, it is good practice for the trainer to provide the trainees with an evaluation questionnaire. This typically asks the trainee to rate a series of statements or questions about the training experience on a very good to very bad scale. This kind of evaluation lends itself to being computerised, so that results can be quickly amalgamated and analysed.

Training evaluation can be beneficial to both the trainer and the trainee. For the trainer, it gives valuable feedback about the effectiveness of the training session, from the perspective of the trainee. For the trainee, a good training evaluation will focus the trainee on how much he or she learned from the training and whether his or her training objectives were attained.

User support

After technology has been installed and users have been trained, there will still be a need for ongoing user support. There will be many occasions where a user will need assistance with a problem occurring during his work.

Typically, user support is supplied at several levels, depending on the complexity of the problem. Support can be provided internally, by staff on site, and externally, by contracted technical experts.

Internal user support

The first port of call for internal user support is usually a help desk facility. The help desk has at least a twofold purpose: to resolve any problems users have with the system and to help the users to employ the system more effectively.

Help desk staff can be either in-house staff or contracted external staff, but the help desk concept is best categorised as internal support as it is generally tailored to the needs of the particular organisation and familiar with its operations.

Many user requests for support from a help desk can be handled by phone. Users can be talked through solutions to problems. In more complex situations, depending on the structure of the computer system in use, where computers are networked, help desk staff or other technical staff may be able to fix problems remotely, from their own computers. In this case, off-site staff can manipulate software and systems used by local users and run diagnostics on their systems to identify faults. These kinds of support are less costly than support provided on site, as problems can be handled without help desk staff leaving their own locations.

However, some problems cannot be fixed remotely, and support staff will be required to provide on-site assistance. Where support staff is co-located with users, this may involve no more than a short stroll down a corridor. However, where support staff is not on site, particularly where an EMB has dispersed offices, provision of on-site support can be costly both in time and money. In this case, maximising the ability to handle problems remotely can help solve problems faster and more cheaply.

One way to maximise the ability to handle problems without on-site attendance by support staff is to train local users to handle common and/or minor problems themselves.

External user support

Depending on the level of internal user support available, for more complex problems, external user support may be required. External support is typically required when proprietary hardware or software needs to be serviced or repaired, or where problems are beyond the ability of internal support staff.

External support tends to be more expensive per hour than internal support. The time taken to respond to requests for external support can also be an issue. External support providers may not be available to fix problems when the EMB would like them fixed, as they have their own priorities. If external support is provided at urgent notice, this usually incurs additional cost.

One way to minimise the cost of external support and to maximise the chance of getting urgent assistance when it is needed is to negotiate a service level agreement (SLA) with an external support provider. Under an SLA, a service provider agrees to provide a guaranteed level of service for an agreed price. For example, different hourly rates can be agreed for responses to problems dependant on the level of urgency involved. In this way the EMB will know the cost of seeking urgent help compared to waiting a little longer, and can make a judgement about whether urgent assistance is really necessary, and whether it justifies the extra expense.

When hardware or software is being purchased, it may be possible to include a guaranteed level of external support in the purchase contract. Most items purchased will include a guarantee of some kind, at least covering quality of manufacture, and statutory provisions may require a minimum level of guarantee.

It is important to be aware of the items and services covered by any guarantee before a contract is signed. In addition to normal guarantees, it may also be possible to negotiate additional support guarantees as part of the purchase price, which may be cost-effective in the long run if ongoing support costs are consequently reduced.

Evaluation and Audit

A good technology management strategy will include an evaluation and audit strategy to ensure not only that the right technology was implemented according to plan, but that it also continues to operate according to plan throughout its useful life.

Evaluation and audit are essentially two sides of the same coin, however they have different emphases. Audit functions generally encompass an element of external or separate monitoring of an organisation or system. Evaluation, while used as an auditing tool, is not restricted to external or separate scrutiny and can be used by managers and users to measure the success of their own systems and improve performance.

Evaluation

Evaluation strategies may be built into the design and implementation strategy of any technology project. What is the technology intended to do? How do we measure whether it is meeting its intended purpose? What outputs of the technology are measurable? What performance measurements or benchmarks can we set?

If evaluation issues are considered before technology is purchased, this will help not only to measure its effectiveness after introduction, but it may also help to clarify whether the technology is appropriate for its intended task.

One of the best ways to evaluate the effectiveness of technology is to set realistic performance measurements and use them. Pitfalls include setting benchmarks that are difficult to assess, and failing to collect or report on those measurements that have been set.

Evaluation procedures may also be built into the routine maintenance and reporting cycle of technology. Relevant managers should be responsible for ensuring evaluation is undertaken and for receiving that evaluation and acting on it if necessary. There is little point in evaluation if steps are not taken where problems are identified.

If problems are identified, evaluation results can be used to develop solutions. After improvements are made a second evaluation can help judge the effectiveness of the changes.

Audit

As with evaluation plans, an audit strategy can be built into the design and development stage of a technology implementation program.

Auditors take the results of evaluation procedures and apply external or disinterested scrutiny to them. The role of auditors in electoral administration is particularly crucial where technology is used for election processes that require transparency and trust. Auditors can serve to validate electoral procedures by providing an independent assessment of the effectiveness of the technology.

Audits can be undertaken by internal or external staff. Where audits are undertaken internally, it is customary for auditors to not have a direct interest in the process being audited, in order to demonstrate the credibility of the audit. Internal auditors can be valuable because they can be expected to know the intricacies of an organisation's operations. However, internal auditors usually do not have the benefit of the credibility that totally independent external auditors can bring.

External auditors have the advantage of having no interest in the outcome of an audit beyond their own credibility and the fees earned. Consequently external auditors tend to have greater veracity than internal ones. Another point in external auditors' favour is that auditing is a skill, and the best auditors are highly trained and very experienced. This kind of expertise may not be held by internal staff unless those staff members are specially recruited for their auditing skills.

External auditors can be used to scrutinise any aspect of electoral technology that is capable of evaluation. In particular, where technology is used for crucial election functions such as recording and tallying votes, external auditors can play an important role.

Computerised systems for recording and tallying votes are only as effective and secure as the computer code used in their calculations. External auditors can be used to scrutinise the code used in these systems and verify that they perform appropriately. Computer code that has been externally audited can then be escrowed, that is, kept in secure off-site storage in an independent authority's control, so that the escrowed version of the code can be compared to the “live” version of the code used for an electoral event. In this way, it becomes possible not only to verify that computer code is free of any hidden flaws or deliberate attempts at manipulation, but also to verify after the code has been used that it has not been changed or tampered with since it was audited.

Minimizing Risks In Using Technology

The use of technology for any purpose may imply serious risks for its users. In the case of electoral administration, a procedural or technological failure may impact gravely on a community, a region or the entire country.

This means that while it is always important to find ways to minimise the impact of technology malfunctions, for electoral administration and especially for voting operations it may be crucial.

Ways to minimise the risks in using technology for electoral purposes include:

- following systems verification, testing and maintenance procedures to ensure that hardware, communications and software operate effectively
- ensuring that the technology is physically secure, preventing accidental damage or unauthorised access
- implementing data collection procedures and methodologies that ensure that data is collected and verified reliably
- organizing appropriate electoral staff training
- ensuring that data and computer programs are secure, including the use of encrypting techniques to prevent unauthorised access
- putting in place data back up procedures, including reliable data storage and restoring
- providing manual contingency systems
- using auditing code and protecting computer software against computer viruses
- taking out appropriate insurance measures to guard against monetary or material loss
- building in performance safeguards to ensure that staff and external suppliers have a direct interest in

the successful completion of a project, such as performance bonds, bonuses or penalty clauses

- adopting public assurance measures to satisfy stakeholders that the technology is reliable and transparent through public logic and accuracy tests, making software code available for scrutiny and conducting voter information campaigns

- adopting and enforcing privacy policies to ensure that personal and confidential data is kept secure, while also guaranteeing that appropriate public information is readily available

Security

One of the most important ways to minimise the risks in using technology is to ensure that the technology is secure. This includes Physical Security, Data Access Security, Software Security and Virus Protection.

Physical security

Ensuring the physical security of technology is one of the main ways to minimise the risks in using technology.

Physical security measures can be divided into two broad categories: security against environmental factors, such as fire, moisture, flood, heat, cold, power failure and animals; and security against human interference, either deliberate or accidental.

Physical security against environmental factors

The types of environmental security measures that can be taken depend on the types of technology being considered and where the technology is used. Security measures appropriate to technology that is designed to travel and/or be used in places with weak or non-existent infrastructures is different from technology that is static and used in office environments.

Where technology is powered by electricity (and most electoral technology is), it is crucial to secure the power source and to provide backup power supply equipment as an integral part of the technology system.

Power can be cut off without warning anywhere in the world. It is advisable to prevent the loss of data during a power interruption by connecting sensitive technology to an intermediary piece of equipment called a uninterruptible power supply (UPS). If the main power supply fails, the battery included in the UPS kicks into operation and power for a limited period during which time backups can be performed, if necessary.

Some UPS systems also issue a warning signal once the main power source fails so that users are alerted to the problem and can take the necessary steps to prevent accidental data loss and conduct a controlled closing down of the system. UPS prices increase with the amount of power they are able to supply, the sophistication of the warning signals and with the period of time they are able to operate.

While power supplies are meant to provide a constant level of electricity, they can on occasion over-supply power. This is called a "spike" and can burn some components of technology equipment. Therefore the use of a voltage regulator between the piece of equipment and the power supply is advisable unless a UPS with a voltage regulator function is in use.

In countries that have unreliable power grids or where power supply can be systematically erratic, intermittent or non-existent, there might be a need to provide a generator capable of powering all the necessary equipment for extended periods. Generators also increase in price with the power they are able to deliver.

Various kinds of generators can be used, powered by various kinds of fuel, typically petrol or diesel and they can be used as the main source of power supply or as a backup when the main power source fails. Generators can be coupled with UPS systems, so that the UPS can handle the transfer from the main power source to generator power.

Where a generator is used as the primary power source, it may be desirable to have one or more backup generators available in case the primary generator fails. Regular maintenance of generators can ensure that they operate effectively.

Another important aspect of physical security is ensuring that technology equipment, particularly computer equipment, is appropriately housed. Ideally, computer equipment is stored in sealed buildings with climate control, so that temperature and humidity are kept at constant, optimal levels, and dirt, dust, smoke and other contaminants are excluded. In many cases, normal building air conditioning systems that control cooling and heating are employed for this purpose.

In particularly harsh environments, however, or in the case of specifically sensitive equipment, normal air conditioning systems may not be sufficient, and special climate control systems may have to be installed. Concentrating equipment in dedicated, sealed rooms, with the climate controlled by a specialised, air conditioning system is one solution. These rooms need to be regularly and carefully cleaned, particularly for dust build-up (dust is attracted by the static electricity generated by computer equipment, especially video display screens).

Cigarette smoke residues can damage computer equipment. Ideally, smoking should not be permitted in workplaces for both the health of workers and their equipment.

It is advisable that equipment used out of doors or in unsecured buildings, such as equipment used by remote polling teams or in polling stations, come with its own secure containers to ensure that outside environmental factors such as dust or moisture do not affect it. It may be necessary to use equipment that is purposely built for use in remote locations, ensuring that it is robust and capable of functioning under adverse circumstances.

Telecommunications equipment also has special physical security needs. In particular, cables connecting computer networks need to be kept safe from harm. Cables are at risk of being gnawed by rodents and being tripped over by humans. Ways of safeguarding cables include shielding the cables inside ducts or strong sheaths, placing them inside walls, below floors and above ceilings, building false floors to enable cables to travel underneath them, burying cables underground or mounting them on poles. Where cables are at risk, alternatives such as microwave links could be considered.

Physical security against human factors

Many of the measures taken to secure technology against environmental factors can also be used to prevent accidental or deliberate human intervention with technology. Physical isolation, such as placing key items of technology like network servers, inside dedicated rooms, can help to reduce the chance of human intervention. Similarly, placing network cables inside walls, below floors and above ceilings makes them hard to access.

However, the most effective physical measure that can be taken to prevent human intervention in technology is to lock the technology inside secure premises. Modern technology has provided a wide range of sophisticated devices that can restrict entry to buildings and rooms to authorised persons only. These include:

- old-fashioned locks and keys
- locks operated by access code numbers (mechanical or computerised)
- locks operated by cards with magnetic strips

- locks that recognise biological features, such as finger prints, hand prints or retinas
- locks that require a combination of two or more of the above methods

The advantage of the more sophisticated locking systems that use computer systems to validate entry is that they can be used to monitor which individuals have accessed a facility and when. Locks that use biological features go one step further and ensure that only identified and verified individuals can enter a facility. Locks that do not incorporate biological features are not as secure since it is always possible for someone to steal someone else's entry card or access code numbers.

Surveillance is another form of security. Security guards can be used to verify entry to a facility. Security cameras can be used by security guards to monitor a range of access areas. Sensors can be used to monitor activity and set off alarms if security is compromised. If on-site security is too expensive, on-call security services can be employed at a lesser rate to patrol the premises from time to time and respond to alarm calls. Alarm systems can be set up that can not only ring a local alarm but can also set off an alarm at a remote security firm or police station.

While locks and surveillance systems are a good form of security, the overall level of security will only be as good as the weakest point in the security cordon. For example, many office buildings allow human access between floors in service ducts (usually for the purpose of providing air conditioning and cable access). It is important to ensure that access restrictions to technology cannot be overcome simply by a person climbing into an air-conditioning access point outside a secure area and getting into the secure area via the space above the ceiling.

If physical security to electoral technology is of high importance, it may be worth employing a security expert to conduct a security audit on the premises to ensure that all appropriate steps are taken.

The final form of security against undue human intervention in technology is to make it difficult or impossible for an unauthorised user to access or change the data held in computer systems. This can be achieved by restricting access to data through use of passwords and encryption.

Data access security

Much of the data held by an election management body (EMB) is sensitive information that is private or privileged and must be kept secure. Many computer programs used by EMBs must be safeguarded to ensure that election processes run fairly and that election results are not compromised by accidentally altered or deliberately sabotaged programs.

Physical security can be used to isolate computer equipment and prevent unauthorised access, but it is only the first line of defence. The next line of defence is data access security.

Password protection

The most common method of data access security is password protection. Several layers of password protection can be imposed. Computers can be set up to require a password before they can “boot up” and give users access to any of the data on the system, either on the computer's local hard drive or on the network. Networks can be configured to require all users to enter a correct user name and password before network access is permitted, so that even if an unauthorised user can operate a local computer they are not able to get onto the network.

Particular software programs can be password protected also, so that even if an intruder can gain access to the network, they cannot run particular programs. Finally, individual files can be password protected, so that intruders are not able to open them even if they gain access to the files or copy them to another system or to a removable disk.

Passwords are not foolproof, however. There are several basic rules that apply to use of passwords, aimed at ensuring that unauthorised users cannot discover them:

- Passwords are best never written down and left where an unauthorised used might find them. If passwords have to be written down, they need to be securely locked away.
- It is beneficial to change passwords regularly—about once a month is a good standard.
- The most effective passwords are the ones that are not obvious—the name of the user, the organisation, a relative, friend or famous person can be relatively easily guessed by others.
- The most secure passwords will contain a mixture of letters and numbers and, if the computer system is case sensitive, a mixture of upper and lower case letters, since such combinations are harder to crack.

- Short passwords are easier to crack—eight characters or more are considered a good length.

- Passwords are best not shared between colleagues, relatives or friends—each person can have their own password.

- In the case of very sensitive systems it may be advantageous for the computer system to keep track of which passwords are used at what times, and what data is accessed.

- It is desirable to limit the number of times in a session when a person can try to enter a password and fail. This is particularly important where password access is permitted on a public network like the Internet (some computer programs can be set up to automatically try huge numbers of possible passwords, if the system permits this).

- When an employee who is assigned a password resigns or leaves a workplace to work elsewhere, that person's password access is best revoked.

- System administrators need the ability to reset passwords for users who forget them.

- Anyone with password access to a computer system (including any externally employed contractors or systems administrators) will need to have a security clearance at a level appropriate to the data accessible on the system.

Limiting authorised access

Even where a user has log-in permission and a valid password, an EMB may not wish that user to access all the data held on the EMB's system. For example, casual staff employed to enter payroll data will have no need to access sensitive election results programs. Password access can be used to limit a user's right to access different parts of a system by applying different levels of access rights to different classes of users.

Where authorised access is provided, introductory screens displayed immediately after logging in can remind users of any legal requirements for maintaining the security of data and of any penalties that may apply to misuse of data.

Data storage locations

Another way to help keep data secure from unauthorised access is to limit the places in which data is stored. In networked computer systems, it is good practice to keep all data, particularly all sensitive data, on centralised servers rather than on local personal computers' hard drives. This practice means that any unauthorised intruder trying to access data has to pass two levels of security to reach data—both the local computers and the network server's. It is generally more difficult to gain unauthorised access to data on a server than it is on a personal computer.

Another advantage of keeping sensitive data on servers is that it limits the number of computers that need a very high level of security. One way to steal data is to physically steal the computer on which it is stored. While it may be too cumbersome, expensive or impractical to keep all personal computers under high security, it is usually highly desirable and more practical to do so with at least the servers.

Remote access to data

Many computer networks allow remote access to data, by connecting to the network over a public system such as the Internet or the telephone system by dial-up modem. This level of access makes it much easier for unauthorised users to access data, because they do not have to gain physical access to EMB premises or a computer linked to the EMB's private network.

A risk assessment can be made to determine whether the level of risk of exposing a network to public dial-up or Internet access is worth the added convenience of allowing authorised users to have remote access. If a decision is made that remote access is needed, a technical expert in minimising the risks of remote access can be employed to ensure that the system is secure as possible. To be most effective it is important to seek up-to-date advice as the technology involved in this area is constantly changing.

Since sensitive networks that allow remote access can be targets for “hackers” who specialise in breaking the security of high profile networks, every possible step needs to be taken to minimise it. One way to do so, particularly if remote access is only needed for a limited range of functions, is to isolate the most sensitive data and programs from that part of the network accessible remotely, so that it is not possible to reach it other than through a local network.

Another way to limit the risks of allowing remote access is to only allow access to copies of data, with no access permitted to the original sets of data.

Firewalls

Firewalls are technological barriers built into computer networks to control access to the networks. Firewalls are intended to prevent unauthorised users from accessing data and programs protected by the firewalls. Technical experts in this field can advise on appropriate firewall technology for a given system.

Audit trails

Audit trails can be used to log the activities of persons accessing sensitive data. Audit trails can show which staff accessed which data, and can also indicate what changes to data were made, when they were made, and who made them. Properly used (and not ignored or overlooked), such audit trails can be powerful tools for either verifying that security breaches have not occurred, or can identify any breaches that have occurred.

Software security

Computer software programs are made up of complex code. Computer programs that perform sensitive operations related to running an election must run correctly, or the success and legitimacy of an election could be jeopardized. For example, should an intruder breach security and get access to software's code, changes could be made that alter the computer-reported results of an election in a way that would be very difficult to detect.

Software security, therefore, is another line of defence in the battle to ensure electoral technology is kept secure.

External auditors can scrutinise the code used in electoral computer systems and verify that it performs appropriately. Computer code that has been externally audited can then be "escrowed," or kept in secure off-site storage in an independent authority's control. This allows for the escrowed version to be compared to the "live" version of the code used for an electoral event.

In this way, it becomes possible not only to verify that computer software is free of any hidden flaws or deliberate attempts at manipulation, but also to verify after the software has been used that its code has not been changed or tampered with since it was audited.

This level of security may not be necessary for all software used by election management bodies, however it is highly useful for crucial systems such as electronic voting and electronic vote counting systems.

Another way of proving the integrity of computer software is using "open source" software rather than proprietary software since code of open source software is publicly available and external programmers can audit the code and satisfy themselves that it performs properly. This may be desirable where competing political participants wish to independently verify software code used for electoral purposes. Whether the advantages of providing code openly outweigh the risks of identifying areas of weakness will be a matter of judgement in each particular case.

Virus protection

Computer “viruses” are a serious threat to all computer systems, particularly systems linked in networks and systems connected to the Internet and to email services. Virus protection software is an essential part of any computer system.

What is a computer virus?

Computer viruses are programs developed by mischievous or malicious programmers that are capable of being attached to software or data files or of being installed on accessed computers to perform a wide range of functions from the benign to the malign.

Benign viruses can simply perform harmless (but usually annoying) functions such as displaying a pop-up message. Malign viruses can corrupt or change data or programs, destroy computer files, or cause massive amounts of email to be generated, threatening the stability of networks by overwhelming them with data.

Viruses are spread by transferring infected or malicious files from one computer to another. This can happen by transferring files to removable data disks, by accessing or downloading files on the Internet or a network, or by files sent by email. Viruses can be executable files (with an '.exe' filename extension) or files in other formats, such as word processing files containing macros. Running these executable files or opening files containing infected macros can cause a computer virus program to run that can potentially do a great deal of damage.

Some viruses take hold of email programs. By accessing a user's list of stored email addresses, a virus can self-replicate itself by sending copies of the virus to each email address. The multiplying effect of this strategy means that a virus can spread to a large number of computers all around the world in a short space of time.

Computers hit by a virus attack can be severely damaged, and a lot of data can be lost or compromised. In the worst cases a computer's hard disk can be rendered useless, and all data on it lost. In this situation the best that can be done is to reformat the hard disk (wipe it clean and start again) and reload all the necessary software from backups.

The possibility of a virus attack is a very powerful incentive to conduct regular, thorough backups of programs and data.

Virus protection software

The way to protect a system against a virus attack is to use virus protection software. Virus protection software is designed to run in a computer either on demand or in the background, so that the user is unaware of it unless a problem arises. Virus protection software is designed to recognise known viruses and prevent them performing their intended functions.

In addition, as new viruses appear frequently, virus protection software is also designed to identify the possible activity of a virus and prevent it from functioning. For example, a typical virus protection program places a “tag” on each known executable file on a computer. If an unknown executable file attempts to run a program, the virus protection emits an alert to the user asking whether the user wishes the program to run. If the user confirms that the executable file appears to be a virus, the virus protection software can delete the virus from the system.

As new viruses are developed, virus protection software has to play a continual game of “catch-up” for each new virus. As a result, virus protection software has to be frequently updated to ensure that it is capable of identifying and dealing with the latest known viruses. A structured regime for updating virus protection software can be part of an EMB’s technology strategy.

Safe computer practices

Regardless of the presence of virus protection software, some viruses can still escape detection and infect a computer system. In order to guard against this possibility, data should be regularly backed up and users should be taught safe computer practices.

All users need to be aware of steps necessary to avoid catching a virus. First, virus protection software can be installed and running, not disabled. Systems administrators will often want to monitor virus software operation to ensure that users have not disabled their virus protection, or users can be restricted from disabling their virus protection.

Second, users need to be careful about opening files and particularly running executable programs if they are not sure that they are legitimately sent by a known source. Even emails from known contacts can be suspect, as viruses can control a user's email contact list and send messages using any name on the list.

Viruses sent by email can be accompanied by plausible and enticing messages that might encourage users to open the infected files. Users need to be cautious of such approaches.

If users are not confident that files or programs sent to them are legitimate they should not open them. If the files or programs appear to be inconsequential, they can be deleted from the computer including from the recycle bin. If the user is not sure whether a file or program is legitimate, the sender can be contacted to verify that the file or program is genuine.

When in doubt, a user is supposed to contact the relevant help desk or technical assistant for advice.

Ensuring Reliability of Data

Electoral computer systems such as voter registers, electronic voting systems, election results systems and personnel management systems are developed and implemented to store and make use of data. Ensuring the reliability of this data is crucially important for any electoral process.

There are several measures that can be taken to ensure the reliability of data used in electoral computer systems.

Use reliable data sources

Methods to collect and capture data need to ensure that the data is reliable and that is not altered in the process. Voter information, for instance, is more accurate if obtained directly from the voters themselves and not from indirect sources such as other organisations' databases, which may be of questionable quality. The most accurate election results data is obtained directly from the polling places or counting centres, instead of media reports, election observers or political parties.

Data capture methods

The next step to consider is the method by which data is captured from the source. Data can be captured in a variety of ways: on a paper form (which could be handwritten, marked with computer readable marks or typed), by telephone (after which the data is usually written down or typed into a computer by an operator), by face to face inquiry (when the data may again be written down or typed into a computer by a staff member), by users directly entering data into electronic forms connected to the organization data centre, by an electronic voting device, and so on.

Some forms of data capture are more reliable than others.

Handwritten forms are probably most prone to error, as handwriting can often be hard to read or decipher. To minimise the difficulty in reading handwriting, persons completing forms can be encouraged to write clearly in capital letters in blue or black ink. Clear writing can also be encouraged by printing forms with guide lines that are designed to make users write each letter or number in a separate box on the form. If it is possible to pre-print any known data about information needed in the form, this may help reduce the amount of handwriting needed and therefore the error rate.

Where data is received verbally by an operator or staff member, appropriate training and procedures can ensure that the operator faithfully captures the correct information. For example, information can be read back to the client to check that it is correct, and the spelling of words checked if appropriate.

Forms that include optical mark recognition devices such as bar codes can be used to simplify data entry and raise accuracy levels. Bar codes can be used to identify the type of form used, where the form was obtained, what the unique number of the form is, and so on.

Data captured electronically, where the data is typed by a user directly into a computer supplied form can be more reliable than data captured from handwritten forms or data taken verbally, as users can be expected to know exactly how their data should appear. However, such data is only as reliable as the user is accurate.

Training of data entry staff

Staff needs to be trained in techniques designed to optimise accurate input and to ensure a safe working environment. For example, regular breaks prevent eye strain and fatigue. Furniture and computer equipment can be situated to ensure good posture and sound ergonomic practices. Distractions such as staff conversation and discussions while entering data can be minimised to ensure input accuracy.

Data verification

One of the best ways to ensure the accuracy of data is to apply data verification techniques. The most common data verification technique (where data is being typed into a computer from a paper record) is to enter every piece of data twice, using two different operators for each piece of data. The results of the two data entries are compared by computer. Any variation is highlighted, and a supervisor is required to make any appropriate correction. This technique usually gives very high accuracy rates.

Double-keying of data can also be used to identify data-entry operators who are not achieving a high level of accuracy. Where under-performing operators are identified, this may indicate that more training is needed or that the operator is not suited to that kind of work.

Data can also be verified by entering the data once, and requiring another officer, perhaps a supervisor, to recheck the data on the computer screen or on print-outs, to confirm that it is correct, or make any necessary corrections.

Using either of the above techniques, it is desirable that data is entered once by one person and then either re-entered or rechecked by a different person, since people can make systematic errors and therefore repeat the same mistakes every time. However, it is less likely that two different people will make the same systematic errors, so a second person is more likely to pick up the mistakes made by someone else.

It is also possible that form design can lead to users or data-entry operators making systematic errors. If significant numbers of similar errors are discovered regularly when a form's data is being recorded, it may be that the design of the form is at fault. Redesigning the form may help to lower error rates in this case.

Some data can also be verified by checks built into the data capture programs. For example, when entering voting places into a database the data entry program may verify the voting place address against a computer table with all valid addresses and accept only those voting places with valid addresses. Such a verification technique does not necessarily ensure that the correct address for the voting place has been entered, but it does ensure that all the recorded addresses are indeed real.

Similarly, arithmetic checks and logic tests can be built into data-entry systems involving entry of numbers so that the data entry operator is prompted to correct the data, the entry is cancelled, an error log is written or any another relevant action is taken. For example, if an operator is entering a polling place voting data, the system can be programmed to query any result that shows more votes counted at the polling place than there are voters registered to vote at that place. Trends can be also calculated by computer systems and any results that vary from the trend by an unusual amount can be identified and queried.

Ensuring reliability of data after it has been captured

Once data has been entered into a computer system, it is important that it be stored securely and maintained, as well as used in a manner in which its integrity is not compromised.

Ensuring availability of data

Once data has been captured and stored securely in a computer system, it must be made available to users in a way that does not allow undue access to the data or the possibility of data corruption.

There are two main components to ensuring availability of data and thereby minimising the risk in entrusting valuable data to technology. These are ensuring that systems operate to deliver data as needed, and backing up data to guard against system failure or data loss.

Making data available

Making data available to users is one of the main purposes of a computer system. At the same time, however, ensuring the integrity of data is of key importance. When dealing with sensitive data, access should be restricted only to those users that need it by using passwords, login permissions or other available controlling mechanisms.

When data can be shared more widely, a difference may have to be made between users that need to access data for information and those that need access to change or update the data. Similar mechanisms, such as password and login permissions can be used to limit those users who are able to change data to those who have a need to do so. In addition, where users are permitted to change data, verification techniques can be used to minimise the chance of errors occurring.

Data backup

The final safeguard against system failure and loss of data is data backup. Regular back up can mean taking these precautions at least once each working day, more often if crucial data is being collected, such as during an electoral event. Data can be backed up on a wide variety of formats and media such as removable disks of various kinds, multiple hard disks, DVDs, and magnetic tapes, to mention a few.

The organisation's overall information technology strategy can document a formal backup regime. Ideally, data backup can be automated to ensure that human error does not cause problems. However, regular checks of automated backups will still be necessary to ensure that computer error does not also cause problems.

“Live” data can be backed up as it is created, by use of mirrored hard disks, which could be located on the same server or on separate servers. Using mirrored disks, the same data is simultaneously stored on two or more disks. This means that if one disk fails, data can be restored from the other. It is preferable to use separate servers for mirrored disks, as a second server can be used if the first server fails completely.

Software programs, both commercial programs and those developed in-house can also be backed-up so that they are available to reload if the production versions of the programs are lost or corrupted. Most programs come loaded on disks. Increasingly, however, programs can be downloaded from the Internet. In this case, backup copies should be stored locally, as there is no guarantee that the same programs will be available on-line in the future. Program disks that are stored in a data library and managed by a responsible officer or staff unit can then be easily located and used if necessary.

Care should be taken, when backing up program data, that software licences are not breached. Most licences include permission to keep backup copies of software.

Manual/Alternative Contingency Systems

One of the surest ways to minimise the risks in using technology is to provide for manual or alternative contingency systems. That way, if the principle technology fails partially or totally, there will be a backup system that can be brought into operation.

An alternative contingency system might be a manual system, but it could also include a backup copy of the same technology, a different use of technology or a different type of technology altogether.

The types of manual or alternative contingency systems that could be used are as varied as the range of uses that can be found for applying technology to the electoral process. Some possible contingency systems could include:

- using stand-alone personal computers or laptop computers with backup data if the computer network fails
- using paper ballots if electronic voting systems fail
- counting paper ballots by hand if electronic or mechanical counting systems fail
- using handwritten scrutiny sheets and hand-held

calculators if computerised scrutiny/spreadsheet systems fail

- using handwritten forms to replace on-screen data capture where computers fail (so that business can continue while the system is down—the data can be entered when the system is restored)
- mirroring computer systems on backup hardware with backup software, in case the main system fails
- ensuring alternative power supplies are available if the main power system fails
- using fax machines, telephones or couriers to transmit election results if on-line systems fail
- issuing printed election results or other information if on-line display systems fail (in a tally room situation, for example)
- ensuring presenters are available and equipped to give "live" presentations if an electronic presentation fails (in a training situation, for example)
- having alternative equipment available on stand-by, so that it can be brought on-line at short notice

Manual or alternative contingency systems will be most effective if they are not implemented as an afterthought, but included in the overall technology strategy from the beginning. The level of resources committed to contingency systems will depend on the level of risk involved. It will also depend on the time-critical nature of the electoral activity. Provision of contingency systems will be most important where the risks are high and the process is extremely time sensitive.

Any equipment or forms needed for contingency systems can be included in the relevant purchasing plan and be available for use if needed during the event. With luck, they will not be needed. However, if they are needed they will be well worth the extra expense.

System Verification, Testing and Maintenance

Three instrumental means of minimizing the risks of technology are system verification, testing and maintenance. Every aspect of a computer system: hardware, software and communications, should be verified and thoroughly tested before the system is used for an electoral event. After successful testing, systems will need regular maintenance to ensure they will perform effectively when they are needed.

The importance of a technology application very likely determines the degree of rigour applied to verifying, testing and maintaining the technology. In the case, for instance, of a crucial electoral function, such as voting, all components of a voting system: hardware, software and communications should be regularly maintained and then verified and thoroughly tested before the system is used for an election.

System verification

For sensitive systems such as an electronic voting system, it is advisable to employ an independent testing office or organization to perform system verification tests, while for any other systems, proper verification and testing procedures can be developed and implemented in-house.

System verification tests or qualification tests may include:

- verifying that all system components namely, hardware, software and communications are capable of performing under expected normal conditions as well as under possible abnormal conditions, including if applicable, storage, transportation, operation and maintenance environments

- verifying that hardware conforms with local environmental requirements, including shelter, space, furnishings and fittings, electrical power supply and relevant extremes of temperature, humidity and pollution

- testing of hardware, software and communications to ensure that appropriate standards are followed and that they perform its intended functions

- performing audits of code

- revision of system documentation to ensure that it is adequate and complete

- testing system security measures to ensure that they are in place, that they are adequate and that they conform to appropriate standards

- verifying that appropriate quality assurance measures are in place

In addition, measures included in a software audit can include:

- verifying that the code is logically correct
- verifying that the programs follow a modular design, meaning that the code is made up of discreet programming modules that can be separately tested and evaluated
- verifying that there is no “hidden” code intended to perform unauthorised functions
- checking that the programming is straightforward, relatively easy to understand and contains code comments to facilitate maintenance by different staff
- verifying that the programming is designed to facilitate testing meaning that it includes code to allow testing of data flow of data within and between modules
- verifying that the code is robust including error treatment routines that prevent the loss of data while identifying, logging and reporting errors so as to allow for a rapid detection and correction of errors
- verifying that code incorporates security features that will prevent unauthorised access and/or detect and control any attempts at unauthorised access
- verifying that the system is user-friendly and does not require complex or obscure procedures that are difficult to follow
- verifying that the software can be easily installed in the live environment
- verifying that the software can be easily maintained, and that errors or defects can be easily identified, corrected and validated after installation
- checking whether the software can be easily modified to add new features

Once all the components of the system are verified, a report is issued and the necessary measures need to be taken to correct the problems found during the verification exercise. Once the corrections take place another round of verification needs to take place.

System testing

After a system has been verified, it needs to be thoroughly tested to ensure that every component of the system is performing in accordance with the specific requirements and that it is operating as it should including when the wrong functions are requested or the wrong data is introduced.

Testing measures consist of developing a set of test criteria either for the entire system or for specific hardware, software and communications components. For an important and sensitive system such as an electronic voting system, a structured system testing program may be established to ensure that all aspects of the system are thoroughly tested.

Testing measures that could be followed include:

- applying functional tests to determine whether the test criteria have been met
- applying qualitative assessments to determine whether the test criteria have been met
- conducting tests in "laboratory" conditions and conducting tests in a variety of "real life" conditions
- conducting tests over an extended period of time to ensure systems can perform consistently
- conducting "load tests", simulating as close as possible likely conditions while using or exceeding the amounts of data that can be expected to be handled in an actual situation

Test measures for hardware may include:

§ applying "non-operating" tests to ensure that equipment can stand up to expected levels of physical handling

§ testing “hard wired” code in hardware (firmware) to ensure its logical correctness and that appropriate standards are followed

Tests for software components also include:

§ testing all programs to ensure its logical correctness and that appropriate design, development and implementation standards have been followed

§ conducting “load tests”, simulating as close as possible a variety of “real life” conditions using or exceeding the amounts of data that could be expected in an actual situation

§ verifying that integrity of data is maintained throughout its required manipulation

System maintenance

After systems have been verified, tested and implemented, they must continue to be maintained to ensure that they continue to perform correctly and that they can adapt to new requirements if needed.

Ongoing monitoring or testing of systems may need to be systematised to ensure that maintenance needs are identified and met when necessary. Where systems are for extended use, a mechanism can be put in place to monitor feedback from users as another means to determine the need for maintenance and modification.

Maintenance routines vary depending on the type and complexity of the technology. Many items come with a maintenance schedule or program recommended by the manufacturer or supplier. For some hardware and software, maintenance is provided by the manufacturer or supplier as part of the purchase agreement.

Where modifications to hardware, software and/or communications are made as a result of maintenance or upgrades, it may be necessary to conduct further rounds of system verification and testing to ensure that requirements meet the same or updated specifications.

Insurance

While insurance may not prevent technology from failing, it can be used to guard against financial loss resulting from the failure of technology. To this extent, insurance is another way to minimise the risks of using technology.

Many government agencies do not take out insurance with commercial insurance companies, preferring instead to be “self-insuring” because it is often more cost-effective to simply cover the cost of any system failure than it is to take out commercial insurance. In some cases, however, commercial insurance policies are purchased by government agencies and an election management body (EMB) may consider whether insurance is an option in accordance with their own local policy.

An EMB considering insuring any of its uses of technology needs to contact appropriate insurance providers to determine whether insurance is available and the cost of needed insurance.

Performance Safeguards

Many election technology projects involve external suppliers of goods and services. These external suppliers may not have the same commitment to the success of an electoral event as an election management body (EMB) has. Inclusion of performance safeguards in contracts with external suppliers can help to minimise the risks in using technology by increasing the commitment of external suppliers to the success of the project. Performance safeguards can also be applied to internal staff to raise their level of commitment to an electoral technology project.

Performance safeguards can include performance bonuses, bonds, penalty clauses and scheduled payments.

Performance bonuses are extra payments above the basic agreed price that are made if agreed performance criteria are met. Bonuses should not be so freely given as to be expected, regardless of performance. Satisfactory performance should be demonstrated before bonuses are paid. Bonuses can be paid at different rates tied to varying levels of performance.

A performance bond is a payment made up front by a supplier of goods or services that is refunded in whole or in part if certain performance criteria are met.

A penalty clause in a contract will provide that agreed performance criteria must be met, otherwise the penalty clause will be invoked. The penalty could include a payment that must be made by the supplier or an amount that will be deducted from payments due to the supplier. Deducting amounts from payment due is probably the most effective kind of penalty clause.

Scheduled or staggered payments on a project are another form of performance safeguard. Payments can be made in instalments as agreed milestones are met, and the final payment on a project can be withheld until the project is successfully completed. This form of payment is a powerful incentive for suppliers to deliver the goods on time and according to the agreed standard.

Performance criteria used to enforce performance safeguards should be clear and measurable. Criteria that are vague or hard to measure can be difficult or impossible to enforce. It will also be most effective if all relevant parties agree to the criteria before the commencement of a project. Furthermore, care should be taken to collect relevant data to ensure that performance can be measured.

Performance criteria can include quality and timeliness measures. Goods and services must be both of high quality and provided on time. Timeliness is particularly important where an electoral event is time-dependent. Timeliness measures are useful to include as performance criteria as they are generally easier to measure than quality measures.

When including performance safeguards in contracts, legal advice may be necessary to ensure that any penalties are legally enforceable.

Encryption

Encryption is an effective tool for minimising the risks of using communications technology whenever there is a need to send sensitive data through a public network or other non secure channels.

Messages transmitted through data communications channels can be subjected to passive and active threats. A passive threat is an intrusion type eavesdropping, whereby an intruder intercepts messages to view the message data. With an active threat, the intruder modifies the intercepted messages.

Basically, encryption encodes data using cryptography techniques in such a way that only the sender and the recipient of the data can read it.

Data is encrypted by the sender using cryptographic algorithms that transform the data appearance but not its meaning. The data that is then transmitted to the recipient does not make sense to an intruder, but the recipient decrypts the data by using similar cryptographic algorithms then transforms the unreadable data back into the original readable data.

There are different types of encryption with different levels of complexity. As with any code, encryption can be broken given sufficient time and resources, although available cryptographic tools that do not need to be kept secret can make it extremely difficult to unscramble encrypted data.

Encryption is supposed to provide data with authentication, integrity, non-repudiation, and secrecy:

- authentication allows the recipient of a message to validate its origin
- integrity allows the recipient to be assured that the data was not modified or otherwise recognize that it was indeed modified during the communication, since modifications cannot be prevented
- non-repudiation can provide the recipient with proof of the data origin by assuring the identity of the sender and/or providing the sender with the assurance that the data was delivered properly
- secrecy or confidentiality prevents disclosure of the data to unauthorized users

Cryptographic algorithms require the data to be mapped, and, at a minimum, require a value called a key to control the mapping process. Given the same text and the same algorithm, different keys produce different mappings, and these keys do need to be kept secret.

Some systems use two different keys to encrypt and decrypt data. The two keys are linked together mathematically. A person's public key is distributed to other users and is used to encrypt messages to that person. The person keeps the private key secret and uses it to decrypt messages sent with the public key.

Data encryption has several uses for electoral purposes. Whenever sensitive data such as personal information or voting data needs to be sent over a public network, it is advisable to encrypt it.

Encryption technology is a rapidly changing field. Therefore, it is advisable to consult an expert in encryption to ensure that the most up-to-date available technology is used.

Public Assurance Measures

Public assurance measures are an integral part of the implementation strategy of any electoral technology that can affect the public. Such measures are another means by which the risks of implementing technology can be minimised.

There are a range of strategies that can be used to assure the public of the reliability of new electoral technology.

Voter information campaigns

Where new electoral technology is introduced, it is important to include the public as stakeholders and to gain their trust in the new system. This may entail a large-scale communications campaign to inform the voting population of the proposed changes.

Before attempting such communication, it may be desirable to use market research methods to test proposals with focus groups or by surveying samples of the population. Significant changes, like the introduction of electronic or Internet voting, may be subject to public inquiries, such as a commission of inquiry or a parliamentary committee inquiry. Public inquiries are a good opportunity to gauge reaction by means of both submissions from the public and the media interest generated by their conduct.

Logic and accuracy tests

Some segments of the public will need more than a voter information campaign to satisfy them that new electoral technology is reliable. These people (such as election candidates, political parties and election reform groups) may need to be convinced that the technology works effectively.

This need can be met by conducting logic and accuracy tests to demonstrate that the technology performs according to specifications, followed by making these test results public.

Code visibility

Another way to satisfy special interest groups of the reliably of electoral technology is to publish the code used for electoral computer programs so that they can be independently analysed. This allows all interested groups to verify, if they wish, that the code being used performs its intended functions.

Where code is published in this way, procedures need to be in place to verify that the code used in practice is the same as the code that has been published. This can be achieved by lodging "escrow" copies of the code with independent authorities, who can compare the escrow copies with the copies used by the election management body and verify that the code is the same.

Publishing code is not routinely done, and is normally only contemplated where a system being used is particularly sensitive, such as an electronic voting or electronic counting system.

Care needs to be taken when code is published, since making it publicly available may expose weaknesses that could be exploited by anyone with access to the code once it is in use.

Public Information and Privacy Policies

Another way to minimise the risks in using technology is to have clear policies concerning what information held by an election management body (EMB) is made public, and what information is kept private.

Many uses of technology are only as good as the quality of the data they contain. This is particularly important for electoral technology, where the data being used is often personal data of electors, as well as voting data.

For electoral data to be accurate, those providing the data need to be satisfied that their personal data is kept secure and that any sensitive data is kept private. On the other hand, those relying on electoral data, such as candidates, parties and election monitoring bodies, need to be satisfied that data is genuine, so some level of public scrutiny is desirable.

These competing needs for privacy for individuals' data and transparency for key electoral data need to be met so that the risks for all concerned are minimised.

Maintaining privacy standards

An EMB can establish clear, written, publicly available privacy standards. These standards could set out:

- what personal information is recorded and stored by the EMB
- what types of personal information are made publicly available (such as names and addresses)
- what types of personal information are not made publicly available (such as dates of birth, identity numbers, and so on)
- whether any personal information not made publicly available is made available to selected organisations (such as law enforcement agencies, social security agencies and medical research bodies)
- whether any personal information is supplied to candidates, political parties or members of parliament

- whether a person has the right to apply to have any personal information suppressed from public release (such as the address of a person who considers publication of his or her address to jeopardize his or her safety, or the safety of family members)
- whether a person has the right to apply to view his or her own private information and then amend any information that may be incorrect

In many countries, existing privacy laws apply to electoral data. However, where there are no legislated privacy laws in force, an EMB might follow its own voluntary privacy code.

Maintaining information availability

While an EMB needs to ensure that sensitive personal information is kept private, it needs also to have a clear policy stating what information held by the EMB is publicly available. Making information publicly available is an important part of ensuring that the electoral process is transparent and open to public scrutiny. Transparency helps to build trust in the overall electoral process.

As with an EMB's privacy policy, an EMB's information policy can clearly set out what information is made publicly available, and what needs to be done to gain access to such information. The list of items that could be made available by an EMB is extensive, and could include everything from that which is designated not sensitive, such as certain personal data, to sensitive internal working documents, such as advice to the government.

Some items that could routinely be made publicly available include:

- electoral roll data (including names, addresses, electoral districts), except for private personal data
- election results (including voting data at all counting levels for all recent elections)
- polling location lists
- electoral laws, policies, procedures and guidelines
- lists of EMB officials
- political disclosure returns

Some countries have freedom of information laws that may require EMBs to make specified types of information publicly available, but where freedom of information laws are not in force, an EMB may need to establish its own voluntary procedures.

Technology can be used to facilitate information availability. In particular, where large amounts of data are made available, it may be more convenient, and more useful, to provide it in an electronic form. Information can be made available on EMB Internet sites, or on CD-ROMs, for example.

Technology for Boundary Delimitation

Technology can be a very effective tool for conducting electoral boundary delimitation, or redistributions of electoral boundaries. Powerful mapping technologies in particular, such as geographical information systems (GISs), as well as database software, can be used by election management bodies (EMBs) to assist with the boundary delimitation process.

The electoral boundary delimitation process can essentially be divided into two categories: determination of political boundaries (such as boundaries of parliamentary districts) and determination of administrative boundaries (such as boundaries of polling divisions).

Determination of political boundaries

Where political boundaries are being determined, there is often an element of "one vote-one value" included in the criteria for boundary distribution, as well as other more subjective criteria such as community of interests, means of communication and physical area. "One vote-one value" criteria generally require EMBs to ensure that either the number of people or number of enrolled electors residing in each district is within a specified range.

The process of drawing electoral boundaries that contain specified numbers of people or electors can be very complex, particularly where the permissible variation from the ideal quota is limited. The process can be complicated still further by requiring projected population growth to be taken into account. For example, for the Australian House of Representatives, a distribution of boundaries for the 51 districts in the State of New South Wales involves ensuring that the number of enrolled electors in each district is within 10% of the quota (or average number of electors in each district) at the time of the distribution, and that the number of enrolled electors estimated to reside in each district in 3 ½ years time is within 5% of the quota.

Technology can be used for this process by keeping track of the number of people residing in each parcel of land, and to allocate numbers of people to proposed districts which are made up of aggregates of parcels of land. "Point and click" boundary delimitation systems can allow EMB users to draw boundaries on computerised maps, which will then automatically calculate the numbers of people contained in each proposed district. This facility saves a great deal of manual calculation compared to "pencil and paper" systems of the past, thereby allowing EMBs to explore many more options than was feasible previously.

Technology can also be used to calculate population projections where distributions are required to take account of population growth rates.

Determination of administrative boundaries

Administrative boundaries are generally boundaries that are not linked directly to political representation on a "one vote-one value" basis. They can include boundaries of polling divisions, which are subdivisions of parliamentary districts that determine where individuals may vote. They can also include local government boundaries that are based on geographical or locality boundaries, rather than boundaries determined by numbers of residents, such as city councils.

Administrative boundaries do not tend to have strict criteria requiring specified numbers of people to be resident in each district. While there is less emphasis placed on determining numbers of residents in each district than there is with political redistricting, technology can still be used for the drawing of boundaries and with printing maps and other related output.

Passive and non-passive systems

It is possible to program boundary delimitation software to automatically draw boundaries according to the applicable criteria. This "passive" method takes the decision-making process away from people and relies on the instructions programmed into the software to produce a reasonable result. While the sophistication of GIS software continues to increase, computerised "passive" distributions are unlikely to produce boundaries that would be free from criticism, except in cases where the position of boundaries is of little importance.

Non-passive software allows the user to specify boundaries, and the software performs the necessary calculations to determine whether the criteria have been met. This method is most widely used as it allows users to draw logical boundaries using their knowledge of the process.

Passive systems can be combined with non-passive systems to provide a computer-generated starting point for users to manipulate as they see fit.

Applications of technology

Some examples of technology used for boundary delimitation purposes include:

- obtaining relevant data, such as demographic, political and geographic data
- defining and manipulating census tracts, or defined geographical areas used for census purposes
- producing maps
- publishing results of boundary delimitation and results of elections following boundary changes
- using GIS to draw district boundaries
- using GIS to evaluate redistricting plans

Using GIS to Draw District Boundaries

Collecting the Necessary Information

Population Data

Maps

Synthesising the Information

Choosing Between Census and Election Geography

Drawing District Boundaries

Redistricting can be carried out using manual techniques - colour markers, paper maps, and calculators - or using sophisticated computers and geographical information systems (GIS) software. The technology employed does not change the task of the redistricters but it does change how the process is conducted and expands the information and options available to decision-makers when a final redistricting plan must be chosen. If GIS is to be used for drawing district lines, the first change in the process is the need to compile an electronic database.

Collecting the necessary information

Redistricting requires the collection of several different types of information. The two essential pieces of information are population data and maps. The population data, which may be in the form of census enumeration data or voter registration data, provide the only means of creating districts that are relatively equal in population. The population data must be associated with specific geographic areas and must be as accurate and up-to-date as possible. Maps are needed to ensure that only contiguous geographic population units are assigned to districts.

If the potential political impact of proposed redistricting plans is desired, then a third piece of information is necessary as well: political data. Political data may consist of statistics on the political party affiliation of electors, if available, as well as election results - tabulations of votes for candidates and ballot measures from previous elections by voting area. Including political data in the redistricting database allows line drawers to produce a political profile of proposed districts and to predict, to some degree, the partisan implications of a redistricting plan.

Election results can easily be entered into the redistricting database, if they are reported for the same geographic unit as the population data. This will likely be the case when the population units for redistricting are based on voter registration data. If, however, the population units are based on a census enumeration, the geographic units for population and political data may not be the same. In that case, census geography and election geography may have to be matched in some manner to create geographic units that can be associated with both population and political data.

Population data

Population data is essential to the redistricting process. Redistricting operates by combining discrete geographically-based units of population to produce districts of relatively equal population. The population data can be either total population counts based on a census enumeration or voter registration data; the geographic population units will therefore reflect either census geography or election geography (these units of geography are often, in fact, the same).

Traditionally the necessary population data has been collected and tabulated by hand. Recently, however, many countries have begun to computerize this data. If GIS software is to be used, population data (regardless of whether it is census enumeration or voter registration data) must be available in electronic form. Furthermore, each reported population count must be associated with a single unit of geography.

Maps

Maps are essential in the redistricting process, but obtaining adequate maps can be one of the most challenging obstacles facing redistricters. While standard maps, such as road maps, identify geographic features and the boundaries of administrative areas such as counties, cities and towns, they may not provide sufficient detail for drawing electoral districts.

If redistricting is based on a census count of the population, then the maps must show the boundaries of the census geographic units for which population statistics are available. If redistricting is based on the number of registered voters, then the maps must show the boundaries of the voting areas for which voter registration statistics are available. The boundaries of the existing electoral districts are usually needed as well as a beginning point for drawing new district lines.

In order to use GIS, software maps must be digitised and available in electronic form. Some redistricters have access to computerised maps because their governments have supported the development of uniform, digitised maps of the entire country and have chosen to make these maps available to redistricters. Digitised maps may be available from other sources, for example: local governments may have compiled digitised maps for transportation, health and other service planning or for land and resource management purposes; utility companies may have created digitised maps for service provision, network management or telecommunications purposes; or private companies may have digitised maps for fleet management, retail site location or for general marketing purposes.

If boundary authorities have access only to paper maps, digitised computer maps of the country can be created, but only at an enormous cost. Of course, these detailed computer maps can be used for many purposes other than redistricting and therefore may be worth the time, effort and expense.

Synthesising the information

If GIS software is to be used to redistrict, a redistricting database must be prepared once the necessary information has been collected. In an electronic redistricting database, spatial data is related to non-spatial information, such as population and demographic data. The spatial data must include the boundaries of the geographic units to be used as the basic building blocks for creating the districts. Population data must be related to each geographic unit. This data may be total population or the number of registered voters for each unit. Additional demographic data, such as population counts by race, ethnicity, religion or language-use for each unit may also be included if useful for redistricting. If the redistricting database is to include political information, then votes for candidates from previous elections should be entered for each geographic unit.

Choosing between census and election geography

Quite often census and election geography are one and the same and choosing between the two is not an issue. In some countries, however, census geography and election geography do not coincide and choices may have to be made. If voter registration data is to be used to create electoral districts, then election geography (for example, polling areas) may be employed as the basic building block for drawing district lines. This geography may correspond to the geographic units for which census data is reported, but it may not. If, on the other hand, census data is to be used, then the geographic units for which census data is reported is usually employed as the basic building blocks for redistricting.

If both census and election geography is available, and the two do not coincide, then the choice of which to use as the basic building blocks for redistricting often depends on who is making the decision. Election officials often prefer that election geography be used as the building blocks for redistricting, since they wish to avoid changing the existing system of voting areas as much as possible. Political parties and incumbent representatives may also wish to use election geography to create redistricting plans because political information is more readily obtainable for proposed district plans if the districts follow voting area boundaries. Regardless of which geographic unit is selected, if both political and census demographic data are desired, and election geography and the population geography do not correspond with one another, they will have to be matched. Matching census geography and election geography can be quite challenging.

Once a decision is made as to which unit of geography will serve as the basic building block for redistricting, a database can be created. This database is composed of spatial data reflecting the geographic units chosen as the basic building blocks, as well as other geographic information of importance such as administrative boundaries (for example, cities, towns, villages), and tabular data associated with these geographic units (for example, census counts and previous election results).

Drawing district boundaries

Once a database has been prepared, the next step in the redistricting process is the formation of districts. The line drawers create a redistricting plan either by assigning geographic units to districts for the first time or by moving geographic units in an existing plan from one district to another. A redistricting plan is complete when all geographic units in a given territory are assigned to a district and all districts in the plan meet the predetermined redistricting criteria. The geographic units to be assigned may be as large as counties or cities and towns, or they may be smaller units of geography such as census blocks or voting areas.

If the line drawers are to create a new redistricting plan by modifying districts in an already existing plan, their tasks may be relatively straightforward. This is especially true if a decision has been made that districts should be modified only as much as necessary to meet equal population standards. If there is no existing redistricting plan to modify or if the number of districts in an existing plan is to change substantially, however, the line drawers' tasks become more challenging.

The line drawing process is an interactive one; the redistricters assign a piece of geography and then determine how the inclusion of that particular geographic unit affects the size and composition of the district. Although aggregating the population totals for the districts after each new assignment is a straightforward process, it can be a tedious one as well. And as geographic units continue to be shifted, this process is repeated over and over again. A plan is completed and ready for evaluation when all geographic units have been assigned to a district.

Although this process has traditionally been done manually with an adding machine or a hand-held calculator, computers and GIS software can automate this process so that each time an assignment is made, the resulting map, population counts, and even political election results, are re-tabulated and displayed immediately on the computer screen. This allows redistricters to access the result of their assignments immediately. Redistricting plans can be created considerably faster and more efficiently and the results can be accessed much more accurately.

Using GIS to Evaluate Redistricting Plans

Many countries have instituted a set of formal rules, or criteria, for their boundary authorities to consider when drawing electoral districts. These redistricting criteria often include stipulations that districts should be as equal in population as possible, taking into account a variety of other factors. Administrative and/or natural boundaries and other geographic features such as sparsely populated or isolated territory are factors commonly listed. Respect for communities of interest is another factor many countries specify. In some countries, especially developing countries, redistricters are asked to consider the means of transportation and/or communication as well. All of these criteria relate directly to the process of creating districts.

Another set of possible redistricting criteria relate to the outcome of the redistricting process—for example, requiring that district plans be drawn so that political parties are fairly represented or that racial, ethnic, religious or linguistic minorities have an equitable chance of representation. But countries that delimit districts usually do not adopt criteria relating to the fairness of the outcome. This is because countries with single-member districts can rarely meet these standards, if fairness of outcome is defined as proportional or near proportional representation for political parties and minority groups.

Regardless of whether the criteria relate to the process or the possible outcome, geographical information systems (GIS) software can often be used to measure compliance with these criteria.

Equal population

The most widely accepted rule for redistricting is that districts should be relatively equal in population. This is because representation by population is a central tenet of democracy and, in countries that employ single-member districts, this rule translates into the principle of equal populations across districts. Districts that are equal in population are necessary if voters are to have an equally weighted voice in the election of representatives. If, for example, a representative is elected from a district that has twice as many voters as another district, voters in the larger district will have half as much influence as voters in the smaller district.

The degree to which countries demand population equality varies. The United States is unique in its adherence to the doctrine of equal population. No other country requires deviations as minimal as the "one person, one vote" standard that has been imposed by U.S. courts since the early 1960s. New Zealand comes closest to that strict standard, with deviations of five percent or less from the electoral quota permitted.

Other countries, while recognising the importance of population equality, have chosen to balance this factor against other redistricting criteria perceived as equally valid. In the United Kingdom, for example, respect for local administrative boundaries is given precedence over exact equality of number. In many African countries, the need to recognise individual tribes may take precedence over population equality. Each country must determine how much variation from the ideal of exact population equality will be tolerated to accommodate other redistricting goals.

Summary reports listing the total population of each district in a redistricting plan is necessary to determine whether a particular plan meets the criterion of equal population, regardless of what level of adherence is required. If GIS software has been used to create the plan, a statistical report listing the population of each district, as well as the percent that district deviates from the population quota, is a very simple matter. An easyclick of the mouse will produce the needed report.

Geographic considerations

In many countries, the electoral laws specify that geography, or certain geographic factors, be taken into account when delimiting electoral district lines. Geographic criteria can be divided into two categories: criteria relating to geographic boundaries and criteria relating to geographic size and/or shape. A boundary authority may be asked to consider factors from either or both categories.

With regard to criteria related to geographic boundaries, for instance, a redistricting authority may be required to respect administrative boundaries such as county and municipality lines and/or natural boundaries created by dominant topographical features such as mountain ranges, rivers or islands. Factors such as the remoteness of a territory, the sparseness of population, or geographic accessibility are common examples of criteria related to geographic size. These factors are particularly important in countries which have large, sparsely populated territories, like Canada, Australia or Russia, or countries with islands or other isolated constituencies that are more difficult to serve. In addition, some countries require redistricters to take into account factors, such as whether the districts are geographically compact.

GIS software enables redistricters to produce maps of the newly created districts instantaneously. These maps allow redistricters to view the configurations of the newly created districts and to overlay administrative, political and natural boundaries onto the new district plan in order to access the degree to which these boundaries coincide with the new district lines. Often, not only is the map of the new districts instantly available, but statistics relating to the size and even the shape of the districts can be calculated and instantly reported. For example, some GIS packages can display the length or perimeter of a district in miles or kilometres as well as mathematical measures of geographical compactness.

Communities of interest

Because electoral districts are usually required to be relatively equal in population, single-member districts often do not reflect distinct geographic communities as signified by municipal, county or other administrative divisions. This does not mean, however, that political representation has been divorced from the notion of "community" in countries that redistrict—many countries that delimit single-member districts continue to emphasise the importance of creating districts that correspond as closely as possible to pre-existing communities, defined as administrative divisions and/or "communities of interest."

The rationale for recognising communities in redistricting is that electoral districts should be more than conglomerations of arbitrary, random groups of individuals. Districts should, as much as possible, be cohesive units with common interests related to representation. These shared interests may be the result of a common history or culture, a common ethnic background, or a variety of other ties that create a community of voters with distinct interests.

GIS software can be used to ensure that previously identified communities of interest are respected if the boundaries for these communities have been digitised and inserted into the redistricting database as a boundary layer. This may be a relatively simple task if communities of interest are taken to be administrative subdivisions, for example, or other regional or local communities that have well-established boundaries. This is more complicated, however, if the boundaries are not clearly defined.

Fairness for political parties and minority groups

Criteria specifying fairness for political parties and minority groups within a country focus on the electoral outcome, rather than the process, of redistricting. Electoral systems that rely exclusively on single-member districts, however, cannot guarantee proportional representation or even some minimal percentage of seats for minority political parties or for ethnic, racial, linguistic or religious minority groups in the population. This is because single-member districts inevitably produce disproportionately fewer seats for minority parties and minority groups, unless these groups are geographically concentrated in such a way that line drawers can create a proportionate number of districts in which these groups predominate, or special electoral provisions have been made to ensure certain minority groups some representation in the legislature.

Another approach to dealing with the inherent disproportionality of single-member districts is to adopt redistricting reforms designed to ensure a fair and impartial redistricting process. Reforms such as the adoption of independent, non-partisan commissions and neutral redistricting criteria do little to alleviate disproportional election outcomes, however. Taking the politics out of redistricting does not mean that a districting plan has no political effect—it simply guarantees that any political bias in a districting plan is unintentional.

Still another means of dealing with the potential political impact of a redistricting plan—and perhaps the most practical approach—is to attempt to determine the likely political implications of a proposed redistricting plan prior to enacting the plan. If political data (previous election results) have been included in the redistricting database, GIS software can use this information to make predictions regarding the likely political impact of a proposed redistricting plan. GIS software can do this by recompiling previous election results to conform with the newly proposed district lines.

Of course, simply being able to predict the likely political impact of a redistricting plan is not enough to ensure that a plan that is as fair as possible to all political groups will be adopted. Only if the redistricting authority is truly non-partisan or if all interested groups and citizens are armed with this information—and can therefore hold the redistricters accountable—can this approach succeed.

If a redistricting authority has a specific political agenda, sole access to this kind of information and/or sole discretion as to what plan to adopt, this information can actually result in a politically biased plan. This may be the reason that many redistricting authorities are not permitted to consider any political data at all when drawing district lines. However, it should be noted that political parties often have access to this kind of information, even if the redistricters do not, and may use this information to influence the boundary authority during the public hearing process. This is one example of why it is important to consider the context under which redistricting plans will be promulgated in deciding whether to use GIS or not.

Requirements for Using GIS Software for Redistricting

Requisites for the use of geographical information systems (GIS) software for redistricting can be divided into the following three categories: computer systems and software, spatial and other data, and users. In addition, a general understanding of GIS and the potential advantages and disadvantages of its use, as well as a frame of reference that permits its use, are important considerations in adopting GIS for redistricting.

Computer systems and software

GIS software runs on the whole spectrum of computer systems ranging from portable personal computers (PCs) to multi-user supercomputers. Regardless of what hardware system is chosen, a number of elements must be considered for the GIS software to operate effectively:

- the computer must have a processor with sufficient capacity (speed and RAM) to run the GIS software and sufficient disk capacity to store large volumes of data;
- a high resolution colour graphics screen to view the output;
- data input devices such as digitisers and scanners if

paper data must be transformed into electronic data;

- data output devices such as printers and plotters.

Hardware requirements are both dependent on and determining of software requirements; hardware limitations may mean that particular software products cannot be utilised, while the availability of software can dictate what sorts of hardware must be purchased.

Software refers to both the operating system and specific application packages. GIS applications run in a variety of operating systems such as UNIX, Windows NT and Windows XP using GIS software programs such as Arc/Info, Intergraph, MapInfo or Maptitude or customised GIS software packages for redistricting.

Cost can be a key factor in the choice of hardware and software. Budgetary constraints, especially in many developing countries, limit the choice of which computer system and software can be used.

Data

Data includes both the cartographic database needed for using GIS applications as well as any accompanying attribute data (primarily population data in the case of redistricting). Data availability and accuracy—and especially the availability of digital cartographic data—are some of the most important requisites for the development of GIS capabilities. The extent to which GIS is used it is often dictated by the availability of digital cartographic data, or more often, the willingness to dedicate resources to creating such a database.

Many countries have produced a complete set of uniform, digitised maps covering the entire country, but others have only begun—or have not yet begun—this process.
Developing countries are faced with a number of limitations in the use of GIS applications that revolve around issues such as cost, training of specialized personnel, and data availability. As needs for resolving questions related to urban and rural land use, transportation, housing, and environmental pollution are emerging, there is a pressure to adopt GIS technology and to develop computerised maps which can then be adapted for use in redistricting.

Users

Users refer to trained personnel able to operate the GIS system. The main requisite for GIS users is the ability to work with computers to manipulate basic GIS software and databases as well as some general geographic and cartographic knowledge in order to be able to use GIS for redistricting.

Many GIS packages are difficult to use without proper training. The language barrier may pose an additional problem as many GIS manuals and programs—especially those designed specifically for redistricting—are written only in English.

Making the Decision to Use GIS for Redistricting

Countries contemplating the use of geographical information systems
(GIS) for redistricting need to give careful consideration to the advantages and disadvantages of introducing a GIS. The reasons for adopting such a system need to be examined, and clear objectives identified.

Issues to be addressed include:

- expected benefits of introducing GIS
- improvement of the efficiency or effectiveness of the redistricting process
- availability of relevant maps
- costs of introducing a GIS for redistricting
- costs of obtaining additional maps

Potential GIS users may find it useful to conduct a thorough cost-benefit analysis to determine whether the expected benefits of adopting GIS for redistricting justify the anticipated costs of implementing and maintaining this technology.

Costs and benefits of using GIS for redistricting

Some of the direct costs that may be associated with the use of GIS for redistricting include:

- acquisition of computer hardware and software
- acquisition of customised software
- hardware and software maintenance and support
- data maintenance, including creating, editing and

deleting data

- hiring of qualified personnel
- training staff

Some of the benefits that may be associated with the use of GIS for redistricting include:

- time saving for routine and repetitive tasks
- faster provision of information
- wider range of information provided
- more accurate information
- new range of output—maps, reports, etc.
- improved quality of redistricting decisions

Some costs and benefits—such as the cost associated with purchasing the GIS system and the time savings benefit—are relatively easy to identify and quantify. Other costs and benefits, however, especially indirect ones, are not as easy to identify and quantify but have to be taken in account when doing a cost-benefit analysis.

The cost of employing GIS for redistricting will vary dramatically depending on the availability of electronic data and the effort required to encode the data if it is not available electronically. If digitised maps of the entire country or of the region under consideration are available, the costs associated with adopting GIS can be expected to be more affordable. On the other hand, if a digital map data base has to be created, and the cost of this cannot be shared with other government agencies or organisations, the effort and cost required may not be worth the anticipated benefits of using GIS for redistricting purposes.

Choosing a GIS software package

Once the decision is made that expected benefits outweigh costs, the next step is to choose a GIS hardware and software.

Various options need to be analysed to determine which one will best meet the identified objectives. This includes deciding whether to develop the software in-house, to purchase a standard GIS commercial package, or to purchase a standard GIS software package and customise it (using in-house staff or consultants). Acquiring a standard, proprietary GIS system is likely to be cheaper, easy to use and well-supported by the provider, but may lack some of the required functionality identified for the specific redistricting exercise.

Some questions to consider when selecting a GIS software package include:

- hardware specifications required to run the software (processor speed and memory, disk storage capacity, storage capacity)
- operating system needed to run the software
- software ease of use
- documentation availability, quality and languages
- training availability
- software vendor market position (assurance of on going development and support)
- availability and cost of software upgrades
- software functions
- ability of software functionality to meet requirements
- extent of software package customisation to meet requirements
- software costs

In addition to researching these questions, a decision-making process may include benchmark tests and/or pilot projects with select GIS packages. For example, a benchmark test might be organised in which three or four GIS vendors are provided with a list of tasks that the potential buyer would like the GIS to be able to perform. The potential buyer might also supply data for use in the exercise. The vendors would then attempt to demonstrate that their system meets the potential buyer's requirements. This exercise requires a fair level of expertise and awareness on the part of the potential buyer, especially regarding the identification of the tasks to be performed by the vendors, but it may be well worth the effort.

Implementing GIS for redistricting

Once a GIS has been selected, it must be implemented. Even if there is nothing technically wrong with the GIS system chosen, problems may arise with its use depending on the how the system is implemented. Factors that could be important to the success or failure of the GIS implementation include:

- commitment to the use of information technology and digital data
- availability of experienced staff and/or consultants
- adequate training to enable staff to operate and support the system, including data entry, creation and maintenance of the GIS databases
- allocation of enough time and resources to create the databases and test the system extensively before being adopted

In addition to choosing the GIS package, ordering the necessary equipment and installing, implementing and testing it, the adoption of GIS technology for redistricting involves a complex interplay of technical and socio-political factors. Therefore, it is important to plan the implementation process carefully in order to ensure that the resources needed for the successful transition from the current to the new redistricting system are in place, that redistricting deadlines are met and that the redistricting plans produced are as accurate as possible.

This effort not withstanding, the risk remains that the optimal redistricting plan may not be created or selected.

Technology for Regulation of Party and Candidates

Technology such as computer office automation software products can be used to assist election management bodies (EMBs) to control the registration of parties and candidates to participate in elections.

The registration of parties and candidates processes that can benefit from the use of technology include:

- party registration, including party member verification

processes and party information databases
- candidate nomination, including nominator verification processes and candidate information databases
- providing information to parties, including voter register data and other general communications
- monitoring and control of party and campaign financing, including candidate/party donations, candidate/party expenditure, public funding and audit

Party Registration

Technology can be used by election management bodies (EMBs) to register political parties for participation in elections. In particular, computer software can be used in the process of determining whether a party has the right to be registered and for creating and maintaining a political party's register.

Party member verification

In many countries, a political party has to meet a minimum membership requirement in order to be officially registered as a party and to participate in elections. An EMB can verify that a party has met this requirement by using software programmed to analyse the party's claims of membership status.

The use of computer software requires party membership data to be captured electronically. In many cases, parties already have digital membership lists, and they are able to provide them to an EMB using an electronic storage media, such as tapes, floppy disks, CD-Rom and DVDs or by email.

Where parties do not have digital copies of their lists, they can usually supply hardcopy lists. These need to be converted into electronic form either by manually entering the data into a database or spreadsheet software, or by scanning the lists using an optical scanner equipped with intelligent character recognition software. If there is a need to digitise signatures or photographs of party members, image scanning can also be used.

Once party membership lists are available electronically, database, spreadsheet or custom made software can be used to process them and produce lists according to various criteria. The software can then be used, for instance, to verify that members are not listed twice or that one person does not appear as a member of several parties twice. By using mail merge software, it is also possible to generate letters , to persons on the membership lists to request confirmation of their party membership. Bar codes can be used on the replies to speed the data entry of responses.

If only a sample of persons on a party membership list is to be contacted in the above manner, software can be used to extract the needed random samples.

Where the EMB has access to a voter's register with digitalised voter signatures, photographs or/and finger prints, signature or bio data recognition technology may be used to verify that the identities submitted as party members are genuine.

Party information databases

Once a party has been registered, the EMB usually requires its details to be kept on file. Database management software is recommended for maintaining this information, although a simple register can be kept on a word processor or spreadsheet system.

Where party register details have to be made publicly available, this can be achieved by providing them in hardcopy and electronic format. Details could be published on the Internet to allow easy access for those with Internet capability. For a large, complex or regularly changing party register, the Internet copy of the register could be linked to the party register database to allow for automatic updating of the Internet version.

Providing Information To Parties

Technology can be used to provide a wide variety of information to parties and candidates.

Information from voters register

Many countries require the election management body (EMB) to supply information from its voters register to registered parties, elected members of parliament and/or election candidates. Where there is a computerized voter's register, this is a relatively straightforward process.

Data from voters' registers can be supplied to parties, members and candidates in hardcopy form or electronic form. Since many voters' registers can contain many names, these registers can be quite large, making hardcopy alternatives on paper or microfiche bulky and costly to produce. Electronic forms of voters' registers are generally cheaper and easier to produce. Electronic forms could include copies written to floppy disk, CD-ROM or magnetic tape, or copies provided by email or downloadable from the Internet.

As voters' registers usually contain personal data, they are often covered by privacy restrictions. EMBs will need to ensure that information from voters registers supplied to parties, members or candidates is supplied in accordance with relevant legislation and guidelines and is protected from unauthorized access or misuse.

The form in which electronic data is supplied to parties, members or candidates might depend on the specific need for the data, the amount of data supplied, and the users' technological sophistication.

Data can be supplied in text, ASCI and Rich Text Format (rtf) format which can be read not only by all the widely used word processing software packages but also by other kinds of software programs as well. Very often, though, data is supplied in one of the proprietary word processing, spreadsheet or database file format that may or may not be read by the users' software packages. If possible, it is desirable to offer the data in a range of formats to suit the needs of the different users.

In addition to supplying voter register data in a simple list format, it may also be desirable (or required by policy or legislation) to supply a software package where together with the data a program is included to work under one of the widely used operating systems that can be used by itself in a computer and dispensing the need for additional software. Such a package can include various database functions, including the ability to search, view and print data based on a variety of criteria.

General communications

Technology can also be used for general communication with political parties and candidates. Emails and faxes can be used to contact parties and candidates quickly and, if necessary, in bulk. Where party and candidate contact details are captured electronically, mail merge facilities in databases and word processing systems can be used to send generic or customized letters to parties and candidates.

Party And Campaign Financing - Regulation and Reporting

Many countries have legislative regulation of party and campaign financing. A typical regulatory scheme might involve public disclosure of campaign donations, expenditure and debts, as well as payment of public funds to parties and candidates for campaign expenses. Some countries also limit the amount of campaign expenditure permitted by candidates and/or parties. Technology can be used to assist with the party and campaign financing regulatory role of the election management body (EMB) or other relevant regulatory body.

Reporting by parties and candidates

Technology can be used to facilitate the reporting requirements of a party and campaign financing scheme. Party and campaign financing reports may require detailed and complex data to be produced. Electronic data capture of report details can greatly assist an EMB in its regulatory and reporting requirements. Electronic submission of data by candidates and parties can also help them fulfil their requirements correctly and expeditiously.

Candidates and parties can submit electronic campaign finance returns using software packages supplied by the EMB or other relevant regulatory body. This software would typically contain electronic forms, with specified fields to be completed. This software could be distributed by disk or email, or could be provided via the internet. The software could lead the party or candidate through the reporting process, ensuring that all relevant fields are correctly completed.

Where parties and candidates do not submit electronic finance returns (either because the facility is not available or the party or candidate is unable to) and hardcopy returns are submitted, the EMB or other relevant regulatory body may still find it useful to electronically capture the data using data entry operators or optical scanning methods.

Auditing of party and candidate campaign finance reports

The EMB or other relevant regulatory body responsible for auditing party and candidate campaign finance reports can use technology to assist the auditing process.

Once reported data has been captured electronically, software can be used to store, sort and analyse the data. Partial amounts can be consolidated into relevant totals. This can help identify whether amounts donated or received have bypassed any legislative thresholds.

Where different entities are required to report their involvement with common transactions (for example, where donors are required to disclose amounts donated and recipients are required to disclose amounts received), reported amounts from one entity can be cross-checked against corresponding amounts from another. Use of mandatory fields in databases can indicate where data is missing or incomplete.

Software can also be used to amalgamate and consolidate reported data, so that data submitted at a local level can be consolidated at regional and national levels to give an overall picture that cannot readily be perceived from the local reports.

Electronic capture of financial reporting can also be used to determine levels of public funding payable for campaign expenses, where such payment is linked to actual expenditure.

Public disclosure of party and candidate campaign finance

reports

The EMB or other relevant regulatory body responsible for auditing party and candidate campaign finance reports is also likely to be responsible for publishing the reported data in a form that can be used by the general public. Again, technology can assist this process.

Electronic capture of reported data and software manipulating of that data can enable the regulatory body to present the data in a consistent format, and to consolidate the data to show regional and national totals that may not be apparent from the raw returns. Data can be published in a variety of formats, including paper hardcopy, CD-ROM, disk and Internet.

Where original hardcopy returns are required to be made public, in addition to providing photocopies, these can be optically scanned and made available on CD-ROM or the Internet.

Candidate Nomination

Technology can be used to assist an election management body (EMB) to process and verify candidates' nominations.

In many countries, a candidate has to be nominated by a specified number of registered voters or by a specified office holder of a registered political party. An EMB can verify that a candidate's nomination has met the relevant criteria by using technology to assist in analysing the candidate's nomination.

In some cases, it may be necessary to record electronically the details submitted with a candidate's nomination or to request the candidate and/or the nominators to supply the data electronically. An EMB could assist with this process by distributing—via disk, email or the Internet—software that is programmed with the necessary forms for the data to be entered into.

Where data needs to be electronically captured but the candidate and/or the nominators are unable to supply electronic data, hard copy nominations are usually supplied. These can be digitalised either through data-entry into the appropriate software or by scanning the lists using an optical scanner equipped with intelligent character recognition software.

Once data has been digitalised, a database management system, a spreadsheet or other customised software may be used to process the nominations. The software can also be used to generate reports or mail merge letters as needed (using also a word processor or a report writer).

If details on nomination forms have to be verified, such as whether candidates or nominators are registered voters, or whether a person shown as a party official is appropriately registered for the purpose, relevant databases or spreadsheets can be consulted.

Technology can be also be used to verify signatures shown on nomination forms. EMBs can assist in this process if they have access to a digitised record of voter signatures (such as a digitised voter register or national identity database where that data is recorded). For relatively small numbers of signatures, an operator would be able to manually compare signatures on nomination forms with signatures on digitised records displayed on screen or printed out. Where large numbers of signatures need to be checked, signature recognition technology might be used to verify that the identities submitted are genuine.

Once all nominations have been accepted, their details are usually required to be made public; digitalisation of nomination information can expedite public disclosure.

There are additional advantages for EMBs to digitalise the candidates’ nomination data. Once this data is stored in a database management system, for instance, it can be linked to other systems that require the same data, such as those used in ballot paper production, election results tallying, public notification and voting place management.

When nomination data has to be made publicly available, this can be achieved by providing information in both hardcopy and in electronic format, including the Internet if available. In this case, it may be useful to have the Internet copy of the nominations data linked to the nominations database to ensure the automatic updating of the Internet version.

Technology for Voter Registration

The process of registering voters and producing voter lists is one of the most important and time-consuming activities carried out by election management bodies (EMBs). Several types of technology can be used for voter registration application, including:

- database management software, for storing and manipulating data
- geographic information systems (GISs), for assigning voters to geographic locations and for ensuring quality and integrity of voter data
- imaging technologies that can be used for data entry

as well as for identification needs, data matching and data recognition

- telecommunications technologies to support networked computer systems and other communication needs

- data storage media, such as disks, CD-ROMS and magnetic tapes

The first step in using technology for voter registration is to determine the requirements of the country voter registration such as:

- centralised versus decentralised
- permanent voter register with ongoing registration versus periodic registration
- the need or not to produce voter cards
- the need or not to use a voter card and a national identity card for voting

This analysis helps determine which available technologies are more appropriate to implement a specific kind of voter register.

Purposes of Voter Registration

When designing an automated voter registration system it is useful to define the purposes of the voter registration process. These would typically include:

- pre-identification of eligible voters (thereby removing the need to prove the identity of voters at the polling place during voting)

- pre-identification of eligibility for candidature (thereby removing the need to prove eligibility for candidature during the nomination period)

- pre-identification of eligibility of members of political parties (using voter registration as means of verifying the qualifications of a political party for registration)

- integrity control (using the voter registration process as a means of preventing multiple voting and impersonation)

- Production of identity documents (such as voter registration cards)

- planning for polling (using the voter register as a means of determining where polling places should be located and how many staff and how much material are needed at each polling place)

- producing lists of eligible voters for use in polling (using the voter register as proof of a person's right to vote)

- identifying names of people who have or have not voted in an election (using records generated during polling based on the voter register, particularly to identify instances of multiple voting and, in compulsory voting systems, instances of failure to vote)

- voter education (using the voter register as a resource to contact electors and to understand the demographics of the voting population)

- providing voter register data to political parties and candidates (as required by law for campaigning and transparency purposes)

- publicly publishing voter register lists (for transparency purposes)

- non-electoral purposes (such as jury lists and sharing data with other government agencies for law enforcement and protection of the public revenue purposes)

These various purposes for which voter registers can be used tend to dictate the form in which voter register data is stored and manipulated. In order to produce this wide range of voter register products, the data contained in voter registers needs to be electronically captured and stored in electronic form, usually in a database system.

A voter register database can be used by an election management body (EMB) to assist various aspects of the electoral process, such as election planning and redistricting.

Voter registration data can be aggregated to various geographic levels to assist with determining where polling places should be located and what resources (both staff and material) should be devoted to each polling place. It may be feasible for an EMB to link its voter registration data with its polling place management database to automatically calculate quantities of material and the number of staff needed. This can be done through assigning “catchment areas” to polling places and calculating the number of voters registered within each polling place's catchment area.

Voter registration data can also be aggregated to various geographic levels to assist with redrawing electoral boundaries or redistricting. Where a redistricting regime requires expected future voter numbers to be taken into account, a voter registration database can be used to plot voter mobility and to determine growth trends over time. However, while voter register data may show trends in growth or decline, care should be taken when using this data for redistricting purposes to include other factors, such as plans for future housing developments or plans to demolish housing.

Voter Registration and the Electoral System

The applicable electoral system and its enabling legislation in each jurisdiction will largely determine what data has to be included in a voter register and what the voter register will be used for.

Voter registration qualifications and disqualifications are generally determined by legislation. The method of applying for registration usually includes the steps an applicant must take to prove eligibility for registration. Such steps can include completing a form with personal data, a declaration of eligibility, proof of eligibility by, for example, providing representatives of the electoral management body (EMB) with relevant identity documents such as birth certificates, passports, immigration documents or a declaration by recognized witnesses if no proof of identity can be provided for a justified reason.

Usually, the electoral legislation determines how an electoral district is defined. This may require that a voter register include voter geographic data to ensure that the voter is registered to vote in the electoral district correspondent to the voter residence address.

Again, these requirements indicate the desirability of electronically capturing and manipulating voter register data.

The applicable electoral legislation is also expected to indicate how the voter register is to be used in the voting process. In most cases, the voter register is used in voting places and EMB offices to determine a person’s right to vote and therefore has to be suitable for voting purposes. This means that copies of relevant information stored in the voter register are available, for instance, in printed hardcopy list formatted in a logical order, so that voter information can be found easily, or in an electronic list accessed by computer. In either case, there is a need to electronically capture and manipulate voter register data.

A requirement to record the fact that a registered voter has voted also impacts on the design of the voter register data base and on how it is used.

The voter data to be electronically captured and manipulated is also determined by additional requirements such as the need to compile master voters lists for the purpose of determining instances of multiple voting or, in the case of compulsory voting systems, instances of failure to vote.

Impact of Voter Registration Methods

The voter registration methods set down in electoral legislation, guidelines or policies will also impact on how technology needs to be used in the voter registration process.

Voter registration can be active or passive. That is, a person may be required to actively apply for voter registration, or a person may be automatically (or passively) registered through participation in another process, such as holding a drivers licence or being included on a national population register.

Where voter registration is active, a process is needed to convert an application into a voter register record. While this process can be conducted using an entirely manual paper-based system, the various outputs required of modern voter registers generally dictate that an application for registration be converted to an electronic form.

Where voter registration is passive, data is generally taken electronically from another source, such as a drivers licence authority or a national population register. This process is generally not practicable without the ability to use electronic data transfer.

Voter identification requirements

Electoral legislation will generally set down what, if any, proof of identity needs to be submitted by a person applying for voter registration. Where proof of identity is required, a system must exist to record the fact that proof has been provided. While a manual paper-based system could be used in this case, an electronic database system would generally be much more efficient.

Where voter identification details need to be recorded and used at a later date for identity purposes, technology can be used to record and store those details. For example, signatures can be scanned and electronically recorded. Photographs can be taken and stored in digitised form. Where digitised bio-identity data is stored, software can be used to determine whether a person has registered more than once.

Types of voter registers

The type of voter register specified in electoral legislation will also impact on the use of technology for voter registration.

A continuous register is a register that is constantly kept up-to-date by amending and adding voter records whenever necessary. An electronic database can be used to easily update records and add new records, as well as keep track of amended and deleted records.

Periodic registers are another option. In these cases, a register could be established for a single electoral event or for any electoral events occurring within a defined period. Periodic registers generally require voters to register anew and previous registrations are not taken into account. While this type of register can be recorded using manual paper-based systems, as there is not as great a need to allow for amendments and updates as with continuous registers, many advantages can still be gained by electronically capturing and storing registration data.

In some jurisdictions no voter register is produced. In this case, voters apply for registration and are given a registration card as proof of registration but no consolidated register is compiled. Where no voter register is produced, the benefits that flow from holding an electronic register are not achievable, and the need to electronically capture data is not present. Therefore, the only benefit technology can give to this process is to assist with the process of issuing voter registration cards. Of all the types of voter registration processes, this is the one least amenable to using technology.

Some jurisdictions do not have a separate voter register, but make use of other government registers, such as a national civil register. In these cases, electronic storage and manipulation is virtually essential in order to manipulate data and produce products that can be used for electoral purposes.

Voter Identification Methods

Technology can be used to assist voter identification processes undertaken by election management bodies (EMBs) during voter registration.

The level of required proof of identity varies considerably between jurisdictions. Some jurisdictions simply require voters to sign a declaration stating their eligibility when registering to vote. Others require voters to provide documentary proof of identity. Some jurisdictions record evidence of identity such as fingerprints or portrait photographs for use during the voting process.

The following topics examine issues associated with voter identification during voter registration:

- identity checks for fraud control
- electronic proof of identity
- technology to verify and record identities of voters

EMBs may issue identity documents or proof of registration documents to registered voters. Technology can be used to automate this process.

Voter register databases can be used to generate the data to be printed on an electoral identity document. Where photographs, signatures or finger/thumb prints have been digitised and stored in a database, they can also be printed on identity documents generated by the voter register database.

Identity documents containing photographs, signatures or finger/thumb prints can also be generated using specialised systems designed to produce identity cards while the subject is present. In these cases, textual information is printed on hardcopy (using data either provided on the spot or data extracted from a database). The voter usually signs this hardcopy record, and/or makes a fingerprint or thumbprint. The operator places the hardcopy printout, including the signature and/or finger/thumb print in the device, and takes a photograph of the person. The device then prints an identity card including a copy of the printed data, the signature and/or finger/thumb print and the photograph. The card is usually laminated and can include tamper-evident security devices such as holograms or embedded print to make it difficult to forge or alter the card.

Identity cards can also be produced that do more than simply show images of text and pictures. “Smart cards” incorporating magnetic strips or data chips can also store electronic data about the person who is the subject of the card. This data can include bio-identification data, so that smart cards can be used with smart card readers and bio-identification readers (such as finger print scanners) to automatically verify a person's identity.

Smart cards can be “read only” cards that simply contain information about the subject. Other types of smart cards can be “read-write” cards, which have the information contained on the card updated as the cards are used. For example, a read-write card used to verify a person's right to vote could, once used, be recorded as having been used for that election, so that it could not be used for voting in that election again.

Where smart cards are used in polling places, they could be used to replace current methods of recording that a person has voted. Where a voter uses a smart card at a polling place to verify his or her right to vote, the smart card reader could at the same time record that that person had voted and transmit that data to a central database during or after polling.

The provision of smart cards to voters and smart card readers to polling places is expensive, so an EMB needs to determine if the advantages are worth the expense.

Smart cards incorporating an electronic identity could also be used for voter registration or voting by computer over the Internet or at a computer kiosk, provided the computer was equipped with a smart card reader.

Computer software can be used to perform a range of tasks that can assist an EMB in reducing instances of fraudulent registration or voting and to identify and delete instances of duplicated voter registration records.

There are various types of techniques and technologies to verify and record identities of voters, namely:

- matching techniques and comparison routines
- signature recognition techniques
- digitized photographs
- bio-identification systems
- identity documents produced by election management bodies
- electronic proof of identity

Proving identity during an electronic transaction emerged as an identity issue in the 1990s and the 2000s. Particularly with moves towards electronic voter registration and voting over the Internet, the issue of proving that the person sending an electronic transaction is the person named in the transaction has become important. Various strategies such as the provision of electronic signatures, public key encryption and the use of Personal Identity Numbers (PINs) are being developed. This field is still in its infancy, however, it is evolving rapidly and improvements can be expected in the 2000s.

Matching techniques and comparison routines

Software can perform various comparison routines to determine whether a person applying for registration is already registered, perhaps at another address. Electronic searches can be programmed into voter registration databases to identify whether a person applying for registration is already on the register. Since people do not always use the exact same name every time they complete a form, software comparison routines need to make use of "fuzzy matching" techniques to help identify possible duplicates. Using fields other than names can also assist, particularly date of birth records. Even with dates of birth, people can show different dates on forms over time, and "fuzzy matching" may also be needed when comparing birth dates.

"Fuzzy matching" involves programming a computer system to search for matching data by applying various criteria. For example, a possible match could be identified where a name differs by only one letter. Possible matches could also be identified where first names and surnames matched but middle names did not match or were absent in one record but not in another.

Names can also be matched using aliases. A system can be set up that compares different variations on the same name, which could be used by a person at different times. For example, aliases for John could include Jon, Jonathon or Johnstone; aliases for Catherine could include Katherine, Caterine, Katerine, Kate, Cate and so on.

Matching techniques also need to take account of people changing names. In some societies, a woman typically changes her surname when she marries. People also change their names by deed poll. Where this occurs, matching by surname will generally not find a match with an earlier record using the old name. In these cases, matches can be found using first name or given name fields and dates of birth. To assist with this process, it is desirable to ask voters on their registration forms whether they have changed their names since their last registration, and to ask for their previous registered address. This data, if supplied, can greatly assist in finding out of date entries.

Fuzzy matching programs often produce several possible matches with a current record, some or all of which may not be actual matches with the person concerned. A human operator should be used at this point to determine whether these are actual matches and to alter the relevant records as necessary.

Signature recognition techniques

Scanning technology can be used to electronically capture handwritten signatures. These digitised images of signatures can be made available to EMB staff over a computer network, so that they can perform visual comparisons of digitised signatures with signatures provided on later documents.

Digitised signatures can also be automatically analysed and compared using appropriate software. This software compares patterns in digitised signatures and can flag possible mismatches for a human operator to investigate.

Digitized photographs

Digitized photographs of people's faces can be used as a method of determining whether one individual has registered more than once. Computer software can be used to compare different photographs to determine whether the same person appears in more than one photograph. This technique could be used for voter registration purposes to determine whether a person had fraudulently registered more than once, if all registered voters have their photographs taken and digitised.

Bio-identification systems

Bio-identification systems can be divided into two main types: visual and electronic.

Visual bio-identification methods include use of photographs, signatures and/or finger or thumb prints on identity cards. These are relatively low cost to implement and administer. Many off-the-shelf identity card issuing systems incorporate inclusion of photographs and signatures. At polling places, polling staff are expected to compare the photographs, signatures and/or finger or thumb prints on the identity cards with the voters.

This process has its weaknesses, as signature and finger print comparison is a highly skilled process that polling staff can not be expected to master, and a person's appearance can often change significantly from that contained in an identity photograph, particularly if the photograph is not updated regularly. Nevertheless, this kind of identity system will probably suffice in most cases where the risk of voting fraud is not unacceptably high.

If visual bio-identification systems are not considered secure enough, electronic bio-identification systems can be used. Electronic bio-identification systems can include digitised voice, hand print, finger/thumb print, or retinal (eye) images. Using these systems, digital records of a person's voice or physical features are stored on disk or smartcard and compared to the actual features of the person using some form of electronic reader. Access is only provided where there is an exact match.

Electronic bio-identification systems are expensive to acquire and administer, and may not be practical for use with the general voting population (although this may change as the relevant technology becomes more widespread and cheaper). However, they are a feasible option for providing security at sensitive locations, such as work places and counting centres.

Voter Registration Processing

The most effective way to use technology for voter registration purposes is to capture voter data and geographic data electronically and store and manipulate the data using a database system.

The mechanics of how to input, store and manipulate voter register data can be a complex process.

The following topics examine various aspects of processing voter registration data:

- The Voter Register Processing Environment
- Database Design
- Processing Functions

Environment

The type of computer system used to process a voter register, and the complexity of it, will depend on:

- the size of the voter population (or number of records) to be stored on the system
- the number of different kinds of data (or data fields) to be stored

- the size of the geographic base to be used in the system
- the number of expected data transactions
- whether the system is to be used for a one time event, or whether it will be used for an ongoing or continuous voter register
- how data is going to be input
- whether the system will store out-of-date records as well as current records (to keep voters' registration history or for auditing purposes, for example)
- how many users will access the system and how often
- whether the system will be used in one office, or whether it will be used in several different geographically dispersed offices
- whether users will expect to access data on line, and whether they will expect data to be up-to-date
- what products will be output from the system
- what hardware the system will be used on
- whether the system will be run on stand-alone computers or over a network
- how data will be sorted and manipulated

A system designed to cater to a relatively small number of voters, to be used in a small central office and that does not have complex input and output requirements will be relatively straightforward. However, where large numbers of voters are to be recorded, and/or where large numbers of users will access the system and/or where complex input and output requirements exist, the voter registration database will need to be more carefully designed and managed to maximise its effectiveness.

Batch or on-line processing

A key decision to make regarding a voter register processing environment is whether to use batch or on-line processing for data input. With batch processing, data is input in "batches" of many records (each record representing a transaction related to one voter) and stored in a temporary data file. At a regular interval (often overnight when the computer system is not in heavy demand), the batched data is uploaded to the main data file, so that new records are added, changed records are updated and old records are deleted or archived in one process.

Batch processing is useful where the available computers are not powerful or are not joined in a network that lends itself to on-line processing of data. With batch processing, any loss of system performance resulting from data updating normally takes place overnight, when system demand is low or non-existent. With some database systems, users need to log out of the database before any updates can be processed, making overnight batch updates a useful method that avoids restricting officers' productivity. Batch processing is also useful where a system is dispersed over different physical networks, so that separate versions of the database need to be updated. In these cases updating each database once a day using a batch update is preferable to updating each database every time a single record is updated.

On-line processing is feasible where powerful computers are used and users share a network capable of allowing on-line updates. In this case, data is entered into the live database rather than a temporary batch file. As soon as an on-line record is updated, it becomes available to other users of the system. On-line processing is more convenient for users as data is kept constantly up–to-date and they do not have to wait for batch updates to be run overnight. However, on-line processing is more difficult to organise as it requires a complex (and usually expensive) network system to make it feasible, particularly where users are geographically dispersed. Special care also has to be taken with database design to ensure that different users are not able to update the same record at the same time, leading to the possibility of errors.

From a usability point of view, on-line processing gives users more current information than batch processing. However, batch processing can be used on less expensive systems and is generally less complex to design and manage than on-line processing. In many cases, the lack of current data using batch systems will not be a significant problem.

Distributed or centralised systems

A complex database like a voter register can be used in essentially two ways: as a distributed system or a centralised system.

A distributed system can be utilized where users of the system are spread over more than one network. In most cases, this occurs where users are geographically separated from other users, such as regional offices in different cities. In a distributed system, each component of the system maintains its own copy of the database and (usually) a subset of the data. For example, in a jurisdiction with six different regions, each of the six regions could maintain data for voters registered only in that region. Whenever there is a need to coordinate data between the distributed regions, this could occur by way of batch updates (see above).

In a centralised system, all the data is kept on one centralised database, which is accessed over a network connecting all the regional offices (if any). Taking the above example, in a jurisdiction with six different regions and a centralised system, users in any region could access data held on any of the regions. Any updates having a cross-regional effect (such as a voter moving from one region to another, leading to a new record in one region and a deleted record in another region) could take immediate effect. In a distributed system, such cross-regional affects would have to wait for a batch update to take effect.

The main advantages of a distributed system include lower costs stemming from less need for high-capacity, cross-region networks, and improved system performance resulting from smaller file sizes, as the amount of data dealt with in a distributed system is less than in a centralised system.

A centralised system, while it is more expensive since it needs greater network capacity and larger file sizes, has the advantages of providing access to all data to all users and of allowing for automatic updating of records across regions.

Database Design

The process of designing databases is a technical skill. Databases are best designed by trained computer professionals.

The design of a voter register database will depend on the complexity of the requirements of the users and of the specified inputs and outputs required of the system.
Factors that will influence the design of a voter register database might include:

- the size of the voter population (or number of records to be stored on the system)
- the number of different kinds of data (or data fields) to be stored
- the size and complexity of the geographic base to be used in the system

- the number of expected data transactions
- whether the system is to be used for a one time event, or whether it will be used for an ongoing or continuous voter register
- how data is going to be input
- whether the system will store out-of-date records as well as current records (so that voters' registration history can be kept and for auditing purposes, for example)
- how many users will access the system, and how often
- whether the system will be used in one office, or whether it will be used in several different geographically dispersed offices
- whether users will expect to access data on line, and whether they will expect data to be up-to-date
- what products will be output from the system
- what hardware the system will be used on
- whether the system will be run on stand-alone computers, or over a network
- how data will be sorted and manipulated

As voter register databases typically contain many thousands of records and may be used by large numbers of users across one or more networks, they need to be carefully designed to ensure they perform satisfactorily. Many strategies can be adopted to improve the performance and usability of a voter register database. Some strategies to consider include:

- choosing an appropriate software platform—off-the-shelf database systems that are supplied with office automation suites are generally not suited to complex databases containing large amounts of data; specialist database software intended for large databases is preferable
- ensure that the hardware used has sufficient processing power and network speed to maximise the

performance of the database

- map out the “architecture” of the database before programming commences (that is, plan how all the different elements of the database will interact before programming starts; this will make for a better finished product)

- use a relational or object-oriented database design to maximise the flexibility of the database

- avoid storage of repeated data by using linked tables and relationships between data (for example, rather than store a complete address for each person in the register, store only a linking address code next to each person, linked to a complete address in a separate address file)

- use computer code that follows industry conventions, so that a person other than the original programmer can correct, modify, update or audit the database.

- document the database, both for users and for programmers, providing user manuals as appropriate and including descriptions of code and fields in the database design to aid programmers

- use standard naming conventions for all the objects in a database (such as tables, queries, reports, forms, code modules, data fields, controls used in forms, and so on)

- use programming code that is of modular design (that is, code that is made up of discreet modules that can be separately tested and evaluated)

- use indexes and unique identifiers (such as a “primary key” to provide a unique identifier for each record) to speed searches and to enable linking between data tables

- use a consistent user interface across the system's range of forms and reports, to increase usability

Ad hoc enquiries

From time to time managers and other users of voter register data may wish to extract data from the voter register database that has not been anticipated by the designers of standard output reports. One way of catering for ad hoc requests is to provide for an on-line reporting facility that permits users to specify a range of variables, such as start dates and finish dates.

Where a user requests data that is not catered for by any standard reports or by a flexible on-line reporting facility, usually the only option left (short of refusing to supply the information) is to ask a programmer to extract the information from the database. This can be an expensive option, particularly where contract programmers are involved, so users should be aware of the cost involved. Where special requests are specially programmed in this manner, it may be desirable to include the request as part of the standard set of reports so that, if the information is requested again, the programmers will not need to be called again.

Data sorting

Usually, whenever data is being used for a report or an output product such as a printed voter register, it needs to be sorted according to logical criteria. Some ways of arranging data include sorting by:

- surname (alphabetically, with a sub-sort on given names, to facilitate finding names on lists)
- *registration number (where it has a logical use, such as where the registration number is used to identify a voter)
- electoral district (usually as a preliminary sort before sorting according to a further criteria, such as surname)
- street number, street name and/or locality (for use in door-to-door canvasses, for example)
- polling division/voting station (for use during polling)
- criteria requested by political players (where they have a right to obtain data)
- data requested for non-electoral purposes (where other agencies have rights to obtain data, such as jury lists supplied to courts, sorted by jury district)

Consideration for likely sorting needs should be taken into account when the voter register database is designed. Some database programs provide for “indexing” of certain fields that might be used for sorting or searching. Indexing fields helps to speed up database performance by recording sort information as the data is stored, thereby reducing the processing time involved when a sort or search is requested.

It may be desirable to include special “sort” fields in a database table. For example, there are various conventions associated with sorting surnames in some cultures. For example, the Scottish “Mac” and “Mc” prefixes are often printed in a sorted list as if they all started with “Mac” to assist users to find names when they are unsure of the spelling. (Therefore, using a special sort field, the following names would be listed as McPhail, Macphee, McPherson, Macphillamy, whereas without a special sort field, a program would automatically sort these names as Macphee, Macphillamy, McPhail, McPherson.)

Random sampling facility

It may be desirable to include a random sampling facility in a voter register database where random samples might be a feature of output products. Database software will usually have a random sample feature that can generate the necessary samples. Where a random sample is required by legislation or other guidelines, an election management body may wish to ensure that the functions can be satisfied by the software before it is purchased.

Some occasions where a random sample facility might be used include:

- jury lists
- selection of poll workers
- research purposes
- verification of party membership lists

Functions

Some of the elements involved in processing data in a voter register database include:

- data creation and maintenance
- data validation
- data reports

The processes of adding, amending or deleting data in a voter register will likely need to be carefully controlled. Safeguards can be enacted to ensure that only authorised users can gain access to perform these tasks, and adequate audit trails can be designed to verify that all additions, changes and deletions are properly made. This is essential to preserve the integrity of the voter register and to guard against fraud.

Data Creation and Maintenance

There are several different elements involved in processing data in an election management body's (EMB's) voter register database.

The methods used to add data to a voter register database depend on the type of data collected (such name, address, birth date, photo and other biometric data), required documentation and the different ways in which voter data can be received meaning personally, by telephone or by e-mail.

On the other hand, data amendment can be required for a number of reasons, including:

- where the voter has notified the need for an amendment (such as a change of address notification)
- where an external agency has notified the need for an amendment
- where the EMB has identified an error in data input
- where an event has occurred requiring data to be updated (such as a change to electoral district boundaries)

The methods used to amend data in a voter register database will also depend on the different ways in which the amendments can be notified.

Data may need to be deleted when:

- new data is received that supersedes old data
- notice is received that a voter is deceased or has left the jurisdiction
- notice is received that a record was created through fraud or error

For transparency and audit purposes, it is usually appropriate to keep a record of data deletions. In many cases, rather than delete data, it is appropriate to move out-of-date data to an archive file where it can be accessed if needed.

In particular, where changes are made to a voter's records over time such as changes to names or current addresses, it may be desirable (depending on local operational and legislative requirements) to keep a history of such changes.

Data validation

Various data validation routines can be applied to data to assist in identifying errors or fraud. Some validation routines that can be used include:

- requiring address data to conform to a standard geographic base
- performing automatic qualifications tests (such as ensuring the voter's date of birth is within the permitted age range or checking that a person's declared citizenship details satisfy the voter eligibility criteria
- checking whether spelling of names conforms to a standard list (thereby identifying possible spelling errors)
- checking whether the number of voters registered at a particular address exceeds the number of persons capable of living at that address
- where signatures, photographs or finger/thumb prints are digitised, electronically checking whether any of these identifying features submitted by a voter matches any other records on the database

It is important that a voter register should only include one current record for each eligible voter, to ensure the register facilitates the democratic principle of one person, one vote.

Software can perform various comparison routines and electronic searches to determine whether a person applying for registration is already registered, perhaps to another address. As people do not always use the exact same name every time they complete a form, software comparison routines need to make use of “fuzzy matching” techniques to help identify possible duplicates. Using fields other than names can also assist, particularly date of birth records. Even with dates of birth, people can show different dates on forms over time, and “fuzzy matching” may also be needed when comparing dates of birth.

“Fuzzy matching” involves programming a computer system to search for matching data by applying various criteria. For example, a possible match could be identified where a name is the same except that one letter might be different. Possible matches could also be identified where first names and surnames match but middle names do not match or are absent in one record but not another.

Names can also be matched using “aliases”. A system can be set up that compares different variations on the same name that can be used by a person at different times. For example, aliases for John could include Jon, Jonathon or Johnstone; aliases for Kate could include Katherine, Catherine, Caterine, Katerine, Cate and so on.

Matching techniques also need to take account of people changing names. In some societies a woman typically changes her surname when she marries. People also change their names by deed poll. Where this occurs, matching by surname will generally not find a match with an earlier record using the old name. In these cases matches can be found using first name or given name fields and dates of birth.

To assist with the data duplication process, it is desirable to ask voters on their registration forms whether they have changed their names since their last registration, and to ask for their previous registered address. This data, if supplied, can greatly assist in finding out of date entries.

Fuzzy matching programs often produce several possible matches with a current record, some or all of which may not be actual matches with the person concerned. A human operator at this point can determine whether any possible matches are actual matches and alter the relevant records as necessary.

Reports

A voter register database should be capable of producing a range of statistical collations of data. This information could be used for a wide range of purposes, including performance management and statutory reporting. Statistical collations are usually produced as reports, which can be printed or made available on-line.

Some examples of statistical reports that could be produced by a voter register include:

- total numbers of voters in the whole jurisdiction, with subtotals for other geographic areas, such as states, electoral districts and sub districts
- total numbers of voters in various voter categories
- total number of transactions processed in the

database, such as additions, deletions, alterations, transfers into electoral districts, transfers out of electoral districts and transfers within electoral districts

- total numbers of voters registered for small geographic areas, such as census tracts for redistricting purposes
- summaries of data from the geographic base, such as types of dwellings, numbers of voters registered at dwellings and numbers of dwellings with no voters registered

Production of some reports can be a considerable load on a database system, particularly where calculations on large data files are undertaken. Such system overload can be prevented or minimized by running complex reports as overnight “batch” requests, that run during system "down times" to avoid overloading the system during peak usage times. Another method is to run routine report requests on a regular basis, often as overnight batch requests, and make those available to users, rather than make on-line requests an option.

Where system resources permit, however, it may be desirable to allow users to have on-line access to reports on demand. This empowers users to receive the specific data they want, when they want it, and can be useful in circumstances where up-to-date information is needed quickly (such as during an election period). On-line access to reports can include user-specified variables, such as start dates and finish dates that allow users to extract customized data.

Targeting groups for special attention

A voter register database can be used for targeting groups for special attention. These might include:

- specific addresses or types of addresses (such as vacant dwellings and institutions, e.g. universities, hospitals, nursing homes, military barracks and flats/apartments)
- societal groups (such as people from specific ethnic backgrounds or people living in remote areas or disadvantaged areas)

Voter Register Data

Voter registration systems reliability and integrity can be maximized by using electronic capture, storage and manipulation of data.
Voter registration system inputs may include:

- paper forms completed by voters
- electronic forms completed by voters
- electronic data provided by other agencies
- hardcopy information provided by other agencies
- verbal advice provided by telephone or in person
- information obtained from field workers in hardcopy or electronic form
- information derived from returned mail

Capturing Data

Before taking a decision on a data capture method, an election management body (EMB) needs to define what data needs to be captured. This data depends largely on the legislative requirements applicable to the voter register, but it can also include requirements specified by administrative and operational convenience.

This means that data only needs to be captured if there is a legislative, administrative and/or operational reason for doing so. It may not be necessary to capture all of the data included by a voter on an applicaton form because some of these fields may be used by EMB staff to determine eligibility to register, but there may be no need to record the data in those fields the register database.

Some voter registration systems for countries with a large percentage of an immigration population, for example, might record on voter registration forms (among other things) the voter place of birth as well as citizenship information for persons born outside the country. This information is used by staff to determine if a person is eligible to register, but once eligibility has been determined there might be no need to store all the related data on the voter’s register for future reference. Another database may be created to archive the digitized images of the original form so that, later on, if necessary, the information can be accessed and extracted.

Data input requirements can be designed taking in consideration the output requirements, which could include, for example:

- data mandated by legislation on voter registration or required by administrative and operational needs
- output fields that could be useful for sorting data or for selecting subsets of data
- special categories that may apply to voter registrations
- needed auditing/tracking fields(such as date and time of data entry or amendment, name of data entry operator, records of previous entries related to each voter)
- output fields needed on the complete range of products, such as assignement of voter to voters stations, statistical and other reports to be derived from the voter register.

Some output fields such as the voter's electoral district can be calculated by the computer software from other input fields like the address fields and do not need to be data entered. .

A typical list of fields captured at the input stage could include:

- name (which can be subdivided into more precise fields, such as first name, middle names, surname and family name as applicable)
- address (which can be subdivided into more precise fields, such as apartment number, street number, street name, locality, district, province, state, postal or zip code and country)
- date of birth
- gender
- former name (if the person's name has changed, for example by marriage or deed poll)
- former address (so that an earlier registration can be cancelled/updated)
- place and country of birth

- identity number(s) (as applicable to the particular jurisdiction, such as ID card number, passport number or social security number)
- citizenship details (for example, if proof of citizenship is required for registration)
- postal address (for those whose postal address is different from their residential address)
- special voter category indicator (for example, a code to indicate whether a voter belongs to a special category of voters, such as a voter whose address is to be suppressed from the public voter register or a voter who currently resides outside the home country)

Capturing hardcopy data

There are two ways to convert hardcopy data into electronic data. The first is to use data entry operators to type or key the data into a computer system. The second is to use optical scanning hardware and intelligent character recognition (ICR) software to convert images into electronic text. Both methods have advantages and disadvantages.

Manual data entry may be preferable to scanning because human operators are generally better able to interpret handwriting than ICR software. Human operators are also able to make decisions about voter eligibility that may not be able to be automated, such as deciding whether a signature looks acceptable or whether the information provided is sufficient. However, manual data entry can be a tedious, monotonous task and lack of concentration can lead to mistakes.

Several measures can be taken to increase the accuracy of manual data entry. A common method is to require data to be entered by one person and then verified by a second person. This verification process can take the form of keying all data twice, keeping both electronic copies separate. The two copies are then electronically compared. If they are both the same, the record is accepted. If they are different, a supervisor can check the record against the original to ensure the record is correctly keyed. Another verification method is to have a second person check the data keyed by the first person against the original form.

Another measure is to design the input screen used for data entry to maximize the accuracy rate. For example, a data entry screen should follow the same logical order as the form being keyed, with design elements used to force the operator's eyes to follow a logical path.

Software can also be programmed to perform logic tests as data is entered to minimize errors. For example, "input masks" can be used, so that only numbers within a specified range can be added in a field where a number is required and only valid dates can be added in date fields. Software can force data entry operators to add valid data to every field, so that fields cannot be skipped or left blank by accident. Where data in a field must conform to a particular standard, such as a defined list of variables, software can reject any entry that does not conform to the standard. Better still, where data in a field must conform to a defined list of variables, the system can offer only those variables, often in a "drop down box" or a "list box". For example, a gender field could allow the operator to only select "male" or "female" as options.

Where data in the voter component of a voter register database is linked to another part of the database, such as the address component of the database, software can force data entry operators to select only a valid address from the address database. Any address given by a voter that does not conform to an address in the address database is rejected by the system, thereby forcing the operator or a supervisor to investigate the legitimacy of the claimed address.

In some cases, the address given may be an unofficial variation of an official address. In others, the address may be fraudulent. If the address turns out to be legitimate but it is not contained in the address database, a separate process should be undertaken to update the address database before the voter registration can be processed, thereby preserving the integrity of the address database.

Data entry using optical scanning hardware and ICR software to convert images into electronic text may be preferable to manual data entry where large quantities of data have to be processed and the process of manual data entry is not likely to add enough value to the process to make it worthwhile.

The biggest drawback with using ICR for data capture is the level of accuracy achieved. Since hardcopy voter registration forms tend to be handwritten, the varying qualities of handwriting can make it difficult for ICR systems to accurately convert handwriting into text, particularly where names are being interpreted, as they do not give ICR software predictable grammatical patterns to follow. However, the accuracy of ICR software is continually improving, and error rates of modern ICR software are much lower than those achieved a few years ago..

ICR software can be effective if the accuracy of the data capture is checked by a human operator against the original form, in much the same way as data is verified using manual operators. This process can be streamlined by software that captures both interpreted text and a picture image of the original form and displays them side by side on screen for operators to check. This method removes the need to refer back to the original forms and means the checking process can be undertaken relatively quickly by a trained and experienced operator.

ICR software is well suited to capturing typed text and can be "taught" to understand various typed or printed fonts with high degrees of accuracy.

Capturing electronic data

Compared with capturing paper/hardcopy data, capturing electronic data is a relatively straightforward process. However, difficulties may arise if the data provided is not formatted in the same way as the data tables into which the data is to be included.

For example, an external agency may provide an EMB with a list of persons who are to be included on the voter register. The voter register will be set up so that data will be included in several defined fields, with each field referring to a particular type of data, such as a surname field. If the imported data does not contain information formatted in the same field structure, the data will have to be converted to fit into the desired structure.

For instance, an EMB may split voters' addresses into separate fields, such as apartment number, street number, street name, locality, state or district, post or zip code. Address data from the external agency might be provided in a "free field" format, that is, the entire address might be typed in one field, with no breakdown of the address into its component parts. In this case, some means must be devised to convert the imported data into the desired format. Unfortunately, this often can only be achieved by considerable manual intervention, making the electronic data exchange a more complicated exercise than it might be expected.

The solution to importing electronic data into a voter registration database is to coordinate data field structures with the agency supplying the data so as to ensure consistency. The best way to do this is to develop an agreed set of data structure standards that can be used across a range of agencies with similar data. Several such standards exist in several countries..

Problems of data structure standards should not arise where EMBs collect electronic voter registration data directly from voters. For example, electronic registration forms provided on the Internet or at computer kiosks can be structured to fit directly into the correct database structure, if practicable.

Electronic voter register data can also be collected by supplying field workers with portable data entry devices. Data can be downloaded from these devices by using removable disks, by connecting the devices directly to a computer or by downloading data over the Internet.

As with manual entry of data, software logic tests can be applied to data captured electronically to identify any possible data errors. For example, any data containing letters in fields that should only contain numbers can be flagged, and operators can investigate the problem and, hopefully, correct it, going back to the source if necessary. Similarly, any addresses submitted electronically that do not conform to the standard address database can be investigated and corrections made as needed.

Capturing data by telephone

In some cases it may be possible to allow voters to register or update their voter register details automatically by telephone, but the opportunities for this type of transaction are rare.

However, it may be feasible (electoral legislation permitting) to accept changes to the voter register by telephone. In these cases, the verbal message must be translated into an electronic form in order for it to update the electronic voter register. This could take the form of a handwritten or typed form completed by the operator, which is then keyed or scanned into the computer system. The advantage of this approach is that it leaves a paper audit trail that can be used to verify the legitimacy of changes to the register.

Alternatively, the operator taking the telephone call could update the register on screen. This has the advantage of saving time by eliminating the step of producing a hard copy record. In this case, the database should record that the change was reported by telephone, so as to leave an audit trail for the change.

Capturing information from returned mail

Where information derived from the voter register is used to address mail to voters that mail may be returned with annotations that may be useful for updating the register. For example, mail that is returned "not known at this address" can be used to annotate the voter register and (dependent on local legislation) either serves to remove the person from the register or to trigger action to investigate the person's right to remain registered.

In other cases, returned mail may indicate corrections to spelling of names or to addresses. This information could also be used to correct the register.

Depending on the type of annotation made on returned mail, the processing of capturing the data on the annotations can be automated to varying degrees. If outgoing address labels include an identifying bar code or identity number or code, that identifier could be used to simplify the data capture of any annotations on returned mail. If annotations fall into defined categories, then data capture of such information can be automated to a high degree. For example, mail containing identifying bar codes that state the voter no longer lives at the registered address could be separately categorised and run through a bar code reader, so as to record the relevant data in the voter register database.

Where annotations show corrections to names or addresses, an operator would be required to key the changes into the electronic register. This process could be speeded up by using bar codes or identity numbers to quickly bring up the voter's record for correction.

Functionality of data entry systems

Data entry systems used for inputting voter register data, from either hard copy or electronic sources, can be designed to perform a range of functions that will add value to the process.

A voter register is typically a continually changing entity, particularly where a continuous register is used. Even where a periodic register is used, changes must be made. A data entry system should permit addition of new records, amendment of existing records and deletion of records. A voter register can also (ideally) be designed to track changes to its records over time, so that a voter's registration history is available.

Voter registers can also be designed to accept data impacting on a voter's record from a variety of different sources, where practicable. For example, a voter's original record may derive from an application form completed by the voter. That voter's address details may be updated at a later date by data provided electronically by another government agency.

Voter Identification

Voter identification is required during two phases of the electoral process: first for registration to establish the right to vote, and afterwards, at voting time, to allow a citizen to exercise their right to vote by verifying that the person satisfies all the requirements needed to vote.

In most countries, the process of voter authentication and verification of identity is done manually, but some countries have implemented and others are experimenting with an automated or at least semi-automated method to verify the identity of voters and their right to vote. This also implies the existence of an electronic voter register. Actually, the technologies used for voter identification at election time depend on the technologies used to establish the voter register.

Most voter identification technologies need to use digitalized voter information and may include the use of:

- smart cards that record a person’s personal information and even biometric data
- database management systems that store and manage digitalized data
- biometric information, such as finger print identification

Smart cards

Smart card technology permits the storage of digital information that can be updated and accessed with an inexpensive reading device that may or may not be linked to a computer network. The smartcard, itself, is a plastic card that resembles a credit card and contains a small chip, which includes memory and sometimes a microprocessor. Gold contacts connect the smart card to the reading device. Since it can store more data than a magnetic strip, a smart card can keep the voter’s relevant data, including biometric data, and can also store non permanent data, such as the polling station where the voter is supposed to vote, for instance. Encryption techniques secure the data, and the tiny processor, if it is there, allows the smart card to be programmed for different applications.

Database management systems

This technology enables the recording, storage and management of required voter data.

Finger printing recognition

While this technology is not new, the electronic methods of recording and recognizing an individual finger print advanced substantially during the last decade of the 20th century. Today, identification can be achieved in a few seconds with reasonable accuracy. As a result, the use of automated fingerprint identification systems (AFIS) that record, store, search, match and identify finger prints is rapidly expanding. AFIS can be integrated in a suite of applications that work together to provide a comprehensive fingerprint and palm print identification solutions to accommodate the needs of voter registration systems as well as voter authentication and voter identification systems used at voting time.

Geographic Information

Data held on a voter register can essentially be divided into two kinds: data related to persons and data related to geography. The geographic base of a voter register is a key element of the register.

The geographic base of a voter register can be used for a wide variety of functions. These include:

- recording the address of a voter on the register
- determining and recording the boundaries of electoral districts
- determining and recording which electoral districts voters are assigned to
- recording lists of habitable and non-habitable addresses (to ensure that voters do not fraudulently enrol for non-existent or non-habitable addresses)
- identifying cases where too many people are enrolled at an address (in order to identify fraudulent or out-of-date entries on the register)
- enabling targeted reviews of the register (by identifying addresses where no persons are registered or addresses with high turnover)
- facilitating reviews of the register (by producing outputs such as lists of names and addresses in street order to facilitate visits by review officers, or the mailing of review letters)
- producing lists of addresses in a variety of electronic or printed form for non-electoral purposes (such as mailing lists for other organisations or for verification of geographic bases held by other agencies)
- There are several different ways in which geographic data on a voter register can be stored depending on the type of voter register.

Name based voter registers

A voter register does not need a separate geographic base (consisting of files containing geographic data only) in order to be functional. A geographic base for a voter register could simply consist of the sum of addresses recorded for each voter on the register. This kind of register can be called a “name based” register, where addresses are contained as fields in records devoted primarily to individual persons (that is, one record per person).

A name based register, however, is an inefficient way to store geographic data. As most addresses usually contain more than one person, a database that stores address data under individual persons' names will contain many repetitions of addresses. Where many thousands or millions of names are stored, this practice will dramatically increase the size of data files and decrease the performance of computer systems accordingly.

A name based register also deprives an election management body (EMB) of the functionality of a combined list of addresses. Such a list can be used to identify anomalies, such as incorrect addresses and fraudulent registrations. It is also difficult to use a name based register to perform other electoral tasks based on addresses, such as redrawing of electoral district boundaries and reviews of the voter register.

Address based voter register

An “address based” voter register generally records addresses in a separate database file (or files) from the list of voters' names. A unique code is assigned to each unique address, and this code is used to link the list of addresses with the list of names on the register.

This approach has several advantages. It dramatically reduces the size of the files contained in the register, as each address only has to be listed once. (With a name based register, each address is repeated for as many people are registered at that address.) Assuming the address register is accurate, it should ensure that voters are registered for valid, habitable addresses. It also facilitates a range of other electoral tasks based on addresses, such as redrawing of electoral district boundaries and reviews of the voter register.

Geographic Information Systems (GISs)

The simplest form of geographic base is a relatively simple text file showing a list of addresses. This could take the form of a list contained in a name based register (see above) or a more useful address based register.

A Geographic Information System (GIS) is a more complex software product that combines text files of addresses with other geographic and spatial data such as maps, aerial photographs, building plans and “spot on the Earth” coordinates.

Developed originally in the early 1960s, GISs are computer-based tools for mapping and analysing data that contain a spatial component. GISs allow users to integrate information, create maps, visualise scenarios and solve complex problems that have a geographic element to them. GIS technology has been applied to a wide variety of enterprises, including environmental and natural resource management, infrastructure planning for transportation and utilities, governmental services and resource allocation, and military and defence planning.

GISs have several different applications for electoral purposes, particularly for drawing or redistricting electoral boundaries.

Geographic data collection and administration

A geographic base is only as good as the data it contains. The data used by an EMB will depend in large part on the data available in that jurisdiction. Some countries will have well resourced government or commercial organisations responsible for collecting and computerising geographic data. EMBs may be able to make use of these resources, if they are available. If these resources are not available, an EMB may have to develop its own collection of geographic data.

An EMB can develop a rudimentary geographic base by extracting addresses from its voter register as submitted by the voters themselves. Depending on the completeness of the voter register, this may be a good start. However, a geographic base derived solely from addresses submitted by electors will have several drawbacks. It will not be complete, as it would be unlikely that persons would be registered for every habitable address, even in countries where registration is compulsory. It is likely to contain errors, as voters often do not use the correct or “official” address of their residence when completing their registration forms. (For example, it is common for people to list unofficial place names as their local address, with the result that voters can give varying unofficial addresses for the same official address.) Perhaps most importantly, it will not be possible to use such a geographic base to determine whether an address shown on a voter registration is fraudulent, since there is no way to independently assess whether an address is accurate.

In some countries it will be possible to obtain or buy a comprehensive geographic base, or a series of them, from other government or private organisations. Local government authorities are often good sources of geographic data. These data sources can be combined into one geographic base for use for electoral purposes. Combining geographic data from a range of organisations can be a complex process. Using defined standards of geographic data is one way to reduce the complexities, but even then differences in use of names of addresses and variation in address numbering schemes can make combining of geographic data a time-consuming process.

Software can be helpful in this regard. Programs can be obtained or developed that will use matching techniques to search for duplicates and identify anomalies.

It may be necessary to conduct fieldwork to compile an accurate geographic base. Staff can be employed to travel around a jurisdiction to ascertain whether addresses listed from the geographic database are accurate, and to identify any missing addresses. The results from the fieldwork can then be entered into the geographic database.

After a geographic base has been established, it will need ongoing maintenance and administration. The data held in a geographic base will need to be updated regularly, as new dwellings are built and old ones demolished. Addresses also change when houses, flats or apartments are subdivided or added to. An EMB will need to keep abreast of changes to addresses by receiving details of changes from responsible government authorities, where possible.

In some cases, the first notice an EMB will receive of a new address might be when a voter attempts to register for the address. In these cases, the EMB will need to investigate the accuracy of the claimed address and attempt to verify it with the appropriate authority.

Geo coding and geo referencing

Every “spot on the Earth” can be defined in terms of geographic code, or “geo code” or “geo reference”. The most common such geo code is latitude and longitude. Several standard geo codes exist. An EMB can consult its appropriate government mapping authority to determine the standard geo code used in its jurisdiction.

Every address in a geographic base can be assigned a geo code. This is a useful practice as it can be used to facilitate data matching of addresses with other organisations that use the same geo code. It can also be used to plot addresses on maps and to allocate voters to electoral districts by calculating the geo codes encompassed within each district.

Geographic Positioning Systems (GPSs)

Geographic Positioning Systems are devices that can plot the precise location of the user, using satellite transmissions to define a “spot on the Earth”. For an EMB's purposes, GPSs can be used by field workers to determine the spot on the Earth of addresses for the purpose of geo coding addresses in a geographic base.

Special address categories

A geographic base used by an EMB needs to be able to allow for special address or voter categories.

Non-habitable or invalid addresses should be identified in a geographic base, to ensure that voters do not fraudulently register for such addresses and to ensure that the geographic base is complete and without any unexplained gaps. Such addresses could include parks, cemeteries and golf courses. Shops, factories and industrial areas may not generally be habitable addresses, but EMBs should be aware that such addresses may still be habitable, since owners, employees or caretakers may reside in them.

While most habitations will be houses, apartments and flats containing relatively small numbers of people, some habitations may legitimately show many people entitled to be registered at the one address. These include institutions, hospitals, universities, military bases, dormitories and prisons. EMBs will need to be aware of these types of habitations and take account of them when using software to identify addresses that appear to have too many voters registered at them.

Geographic bases will also need to account for vacant dwellings, including dwellings where no one resides and dwellings that are vacant in the sense that no persons are registered at them. For the purposes of reviewing the accuracy of the voter register, vacant addresses can be targeted to ascertain whether anyone should be registered at those addresses. It is generally desirable to include vacant addresses in the geographic base so that they can be identified as valid addresses should a person apply to be registered at that address in the future.

Special voter categories

A comprehensive voter register will be able to cope with voters who do not have addresses that fit neatly in a geographic base. Depending on the applicable electoral legislation, voters may be able to register without having a permanent address. These categories of voters might include homeless people, itinerant people who move frequently and have no permanent resident, and those people living outside the country or district who retain an entitlement to be registered. These categories of people will need to be assigned a notional geographic attachment with a particular constituency, to enable their eligibility to vote for a particular district to be ascertained.

Linking addresses with electoral districts

A geographic base will be capable of linking voters' addresses with electoral districts. This will enable the production of lists showing eligibility to vote for particular districts as well as facilitate the redistricting process.

When electoral boundaries are altered by redistricting, a process needs to be in place to update the register to reflect the new boundaries.

Addresses can be linked with electoral districts by assigning each address with a “spot on the Earth” indicator such as geo code, and defining each electoral district in terms of the “spots on the Earth” or geo codes included within it.

Where a unique geo code is not available for each habitable address, addresses can be linked to electoral districts by assigning each habitation to a small geographic unit, such as a census tract or a municipal authority district. Electoral districts can then be defined in terms of the smaller geographic units they contain in order to allocate habitations to them.

When taking the approach of using small geographic units such as census tracts to assign habitations to electoral districts, care needs to be taken where an electoral district boundary divides the geographic unit. In these cases, an EMB will need to determine on which side of the boundary each habitation is located in order to decide which electoral district should be assigned to the habitation. In some cases, this can be done using maps; in other cases a field inspection might be necessary.

Technology for Reaching Voters

Technology can be a very effective tool for reaching and informing voters of issues related to elections. A wide range of different technologies can be used by election management bodies (EMBs) to communicate with voters.

The different applications of technology that can be used to reach voters include:

- informing voters about technology by using demonstrations and simulation exercises, onsite training and websites

- audio visual applications, including radio, television, film, audio tapes, video tapes, DVD, cinema, laser/hologram and multimedia
- telephone communications, including telephone information services, call centres and interpreter services
- automated direct mail
- Internet, including email publication, web publishing and interactivity
- computer kiosks
- desktop publishing
- technology for special needs groups, including the ones used by language services, hearing assistance and visual assistance

Technology can also be used as a means to inform voters about electoral technology used for voter registering and voting. This can address two important issues: the need to educate voters on how to use technology during the voting process, and the need to gain the voters' acceptance of and trust in the technology.

Voter education is often approached as a voter training exercise, but given the number of voters, it may be sometimes more effective to reach the voters and inform them using the communication technology available rather than using more typical training techniques.

Since new electoral technology may affect the public, it is also important to include the public as stakeholders in the process and to gain their trust in the new system. This may entail a large-scale communication campaign to inform the voting population of the proposed changes.

Voter education

Before attempting any large-scale communication campaign, it may be desirable to use market research methods to test the proposals and its efficiency. Voter education needs are very different from staff training needs, and therefore the training opportunities can be also very different.

On the other hand, as with staff training, the complexity of the education depends on the complexity of the technology being used. As voters cannot be expected to master complex technology, it is very important that the technology used by voters is simple and easy to use in order to facilitate voters' education.

There are several ways to educate voters about voting technology. Before voters reach the polling place, they can be reached by mass communication techniques, such as television, radio, newspapers, mail, posters and technology demonstrations. An intensified voter education effort may be especially useful where a new or unusual technology is being introduced, such as a new electronic voting system, for example.

Nevertheless, while mass communication can be used to inform voters about a new technology that is being introduced and to make known what to expect at the polling stations, it may not be sufficient for training people on how to operate technology.

This means that additional technology training may have to be provided right where it is being used by the voters in which case there may be different training options to consider.

The best option remains to provide technology that is as simple and self-explanatory as possible. Where the technology is screen-based, the screens can walk the voters through the process with simple on-screen instructions that capitalize on knowledge that many users already have, such as the use of the "enter" and "cancel" buttons, for example.

Where on-screen instructions are used, facilities need to be in place for people who might have difficulty reading them. Some people may not be able to read well or at all; others may not be able to read the national language well or at all, while others may be sight impaired or blind. Some options to consider include:

- using audio instructions (perhaps via headphones)
- using keypads with touch-readable keys
- providing instructions in a range of languages
- keeping instructions clear and simple
- providing the facility to increase the size of printed instructions
- providing staff in the polling place who can assist voters having difficulty

Other options for training voters in polling places include explanatory posters and demonstration opportunities. For example, a demonstration system could be set up at the entrance of a polling place to allow voters to try out an electronic voting system, with staff available to explain the system, before the voters proceed to complete the real thing. Audio-visual presentations could also be used at polling places to provide instructions on using technology.

No matter what primary method of voter training is used, it is advisable to provide staff in the polling place that can assist any voters who need help. There will always be some people uncomfortable with or unfamiliar with technology who will appreciate the help of a person.

Another way to reach voters is via the Internet. Information can be delivered about a wide variety of election-related topics, including elections and technology. In addition, demonstration sites can be set up to let voters try out new technology interactively, if the new technology lends itself to Internet training. However, this is unlikely to replace other mass communication techniques since, on one hand, it requires the user to be motivated enough to visit the Internet site, and on the other hand, most Internet users are likely to have relatively good technology skills and thus not need the training.

These considerations not withstanding, it may be useful to provide training or assistance to voters by Internet whenever they are able to vote from home and avoid voting places all together.

Beyond the Internet, voter education can be made available through a telephone "help desk" or call centre facility, where voters can talk one-on-one with a trained operator about using voting technology or other voting concerns.

Audio Visual Applications

Audio visual applications are widely used by election management bodies (EMBs) to reach voters.

Common audio visual applications include radio and television programs, publications using audio tapes, video tapes, compact disks (CDs) and digital video disks (DVDs), cinema, lasers/holograms and multimedia activities.

Preparing audio video material for public distribution is a difficult task. Skilled, professional advertising companies, audio-visual companies and/or broadcasters are often the best choice for preparing audio visual material for broadcasting or distribution. While these services may be expensive, the difference in quality between professional and amateur audio visual material can make a big difference in the effectiveness of the material.

When using audio visual technology to reach voters, it is advisable to use a mix of different methods. No one audio visual technology can be considered the only effective media to be used and there is a need to maximise the impact of an EMB's information campaign.

Television and radio are traditionally the most used and most effective audio visual technologies for informing voters. The relative weight given to television and radio broadcasting depends on the local patterns of use of these media. In some countries, television has a greater impact than radio in reaching audiences. In other countries, radio has a greater reach. Advertising agencies can advise on the market reach of the various broadcasting alternatives available, so that an EMB can judge where best to spend its resources.

Radio

Public broadcast radio is extensively used in many countries for electoral advertising. It is relatively inexpensive and it has the potential to reach a wide audience. Radio advertising is particularly useful for audiences who have difficulty with printed material for literacy or disability reasons.

Public radio is also particularly effective in culturally diverse countries where several different languages may be spoken. Alternative radio stations are also a way to offer a wide range of broadcasts in various languages that can appeal to people from a variety of cultures. Radio is also increasingly being broadcast on the Internet, expanding its reach around the world for those with access to the Internet.

The wide range and reach of public radio broadcasting makes it a very important tool for communicating electoral matters.

Television

Publicly broadcast television is widely used by many electoral authorities for electoral advertising. Like radio, it has the potential to reach a wide audience and is useful for audiences who have difficulty with printed material for literacy or disability reasons. It also has the added benefit of using images as well as sound, making it a very powerful medium. However, television advertising tends to be expensive.

Audio tapes/compact disks

Recordings of electoral material on audio tapes and/or compact disks (CDs) are a relatively inexpensive way of reaching voters who have special needs or who do not have access to public broadcast radio or television. Tape and CD players are relatively cheap and widely available in many societies.

Material recorded on tapes and CDs could simply be copies of material designed for broadcast on radio. However, unlike radio which is generally restricted to short messages of a minute or two maximum, tapes and CDs can include additional information for little extra expense.

Material recorded on tape and CD can also be tailored to special audiences, in a way that would not be practicable for radio broadcasting. For example, readings of detailed electoral information contained in printed material can be recorded on tape and CD for voters who are unable to read the printed material for disability or literacy reasons.

Video tape

Electoral material recorded on video tape has similar virtues to material recorded on audio tape or CD but with the added advantage of providing visual information. This means electoral messages can be conveyed using images as well as sound. Analysis of the effectiveness of communication methods indicates that many people learn better by seeing information compared with only hearing it, making video recordings a powerful learning tool.

Video recordings can include the same material used for broadcast television, but, as with radio versus tape and CD recordings, the lower price of video production and distribution means that much more information can be included on a video.

Video is particularly useful in countries with poor television facilities, where videos tend to be more widely accessible. The challenge for EMBs in these situations is to distribute videos effectively so that target audiences are reached.

Video is also a very useful tool for electoral education taking place in schools and other community groups. Videos can be used in electoral education facilities, if they exist, or for electoral education sessions held in schools, community centres and the like, either presented by EMB staff or by local teachers.

Digital video disk

DVD technology is relatively new, and the reach of people with DVD players at the beginning of the 21st century is still relatively limited compared to people with access to audio tape, CD, and video players.

DVD recordings can combine the virtues of audio, video and multimedia presentations in a portable format similar to CD recordings.

Cinema

Cinemas can be used for communicating electoral information to voters in a similar fashion to television advertising. The effectiveness of cinema advertising compared to television depends on the local audience reach of cinema compared to alternative media.

Lasers/holograms

Lasers and holograms are comparatively specialised uses of technology for communicating electoral information. Lasers and holograms can be used for dramatic effect in presentations and displays in electoral education facilities. For example, lasers and holograms can be used as part of pre-recorded multimedia presentations for school groups. In Canberra, Australia, lasers and holograms are used by the Australian Electoral Commission at its electoral education centre to give the appearance of live miniature presenters talking and interacting with props in presentations for school groups.

Multimedia

Multimedia material can be distributed on CD-ROM, DVD and the Internet to give a more interactive, non-linear form of information presentation compared to radio, recorded audio, television or video material. Multimedia material, which generally has to be run on a computer equipped with speakers, combines audio, still images and moving video images with the flexibility of a computerised presentation to present users with an informative, entertaining medium.

Multimedia material can give the user the option of viewing material in an order chosen by the viewer, rather than a specified linear order, as is the case with television or video material.

Multimedia material is well suited to convey complex material and is particularly useful for school students’ electoral education. However, it is relatively expensive to produce, and an EMB needs to decide whether the expected return on using such material is worth the cost.

Telephone

The telephone can be an important part of an election management body's (EMB's) strategy for reaching voters.

Telephone call centres

During an electoral event, teams of people in telephone call centres can be employed to handle large numbers of calls from the public. Database inquiry systems can be used by call centres to enable casual staff to handle relatively complex inquiries and to keep records of the number and type of calls.

Special national toll-free or low cost telephone numbers can be used and advertised widely. These generally easy to remember numbers enable the public to telephone a call centre from anywhere in the country for no or minimal cost—the cost of the calls are covered by the electoral authority.

Pre-recorded touch-tone services

Telephone information lines can also be automated (sometimes called touch-tone services), so that callers can listen to pre-recorded information. Menus of information can be presented to callers, who can select items from the menu by pressing numbers on their telephone number pad. This system reduces the number of staff needed to take phone calls and ensures that information is provided in a consistent form. An option is usually given to allow a caller to speak to an operator if the caller is not satisfied by the recorded messages. This method is particularly useful when large volumes of calls are received and when callers tend to have a predictable range of enquiries.

Usage of pre-recorded telephone information lines by government and commercial organisations increased significantly in many countries in the 1990s, often in an attempt to lower costs by reducing the number of telephone operators. However, they have tended to attract a considerable amount of criticism from users who would prefer to deal with "real people" rather than pre-recorded messages. This criticism can be well deserved where users are forced to navigate a confusing array of menus and sub-menus before they are able to access the information they want or are given the option of speaking to an operator. To avoid this kind of criticism, an EMB considering the use of pre-recorded messages can strive to keep menus simple and straightforward and provide an option to speak to an operator early in the menu structure.

Telephone services outside election periods

Outside an electoral event period, when the number of callers to an EMB is likely to drop significantly, there may be no need for a dedicated call centre or pre-recorded information line. However, the telephone may still remain an important source of contact between an EMB and the public. An EMB may need to ensure that it maintains a telephone information service capable of responding to the expected number of calls, which may simply involve assigning telephone duty to relevant permanent staff.

"Smart" telephone technology

Both in and out of an electoral event period, telephone inquiry services can benefit from various "smart" functions now available in telephone technology. Automatic call diversion technology can be used to ensure that a caller never receives a "busy" signal. Instead, incoming calls can be directed to the next available operator. In the case of an EMB with several different offices that likely spread across several regions, automatic call diversion technology can be used to divert the call to an operator in any office where an operator is free. This enables workloads to be spread across different offices and can relieve the pressure on a particularly busy office while ensuring that clients' calls are promptly answered.

Other "smart" telephone functions that could be used by an EMB include answering machines, call forwarding and call waiting functions. The local telephone service provider can advise on the availability telephone service functions.

The range of new services that are becoming available on mobile phone networks such as Internet access and email services are substantially improving communications in otherwise very isolated places.

Telephone interpreter services

The telephone can be used to provide interpreter services in some countries. Such a service allows a person to call a designated number and ask to speak to a person in a particular language. The interpreter service will connect the caller to an interpreter who speaks that language. The interpreter may be able to answer the call himself or herself (and may be provided with information for that purpose by an agency employing that service), or may set up a three-way conference call involving the caller, the interpreter, and a person at the agency that is able to answer the inquiry.

An EMB can make use of telephone interpreter services to complement its telephone information line. The telephone number of the interpreter service can be included on material published by the EMB, accompanied by instructions to call the number for further information in a number of languages.

Automated Direct Mail

Automated direct mail is another way in which an election management body (EMB) can use technology to reach voters.

Automated direct mail is made possible by the electronic storing of name and address data in databases and/or spreadsheets. Word processing or database software can then be used to print personalised mail to those listed in an electronic mailing list.

By sorting the data according to specified fields, direct mail can be personalised and targeted for each recipient. For example, where electoral boundaries have been redrawn, an EMB could use its voter registration database to write personalised letters to all registered voters whose electoral district has been changed and inform them of their new district.

The content of automated direct mail can be altered according to criteria specified by the user. In the above example, the direct mail was personalised to indicate each voter's own district. In other cases, the text of letters can be changed to take in account particular circumstances by using data contained in the mailing list database. For example, details of special electoral registration criteria applicable to individual cases can be varied in each letter according to each voter's enrolment registration category specified in the database.

It is usually practicable for an EMB to print small quantities of direct mail letters in-house. However, where many hundreds or thousands of letters are to be printed, it is often preferable to have the letters printed by a commercial mailing house. In this case, it is generally possible to supply the mailing house with the relevant database and master mail merge documents on disk or by email with instructions for how the mail merge is to be conducted. The mailing house should then be able to print the letters using the EMB's digital data. In this case, it is a good EMB practice to check proofs of the merged data before the print run and the mailing takes place to ensure that everything is correct.

Some commercial mailing houses are able to add value to automated direct mail by including several attachments or enclosures with mail merged letters. This can include simply a standard enclosure with a letter or, in the case of more complex routines, particular letters can be coded to receive particular enclosures. For example, where an EMB has different enclosures targeted at voters registered in specific electoral districts, a mailing house can use a computerised insertion process to include the enclosure specific to each voter's electoral district.

Internet

Internet web sites are excellent means of conveying large amounts of information to voters compared with traditional communication methods such as printed media, brochures, radio and television, which are able to carry only a limited amount of electoral information. In an ever growing number of countries where

Internet facilities are widely available, election management bodies (EMBs) can greatly expand their information delivery capabilities by including references to their web sites in their paid advertising. Web sites can be structured to deliver as little or as much information as the user desires.

In addition to delivering information, electoral web sites can also be interactive. Users can complete transactions on-line, such as applying for voter registration or voting away of voting places. Forms can also be completed on-line, such as campaign finance disclosure returns, or they can be downloaded for printing on the user's printer and returned by mail (particularly where a user's hardcopy signature is required).

EMBs need to be careful that provision of information and services on their Internet web sites does not discriminate against or unfairly disadvantage clients who do not have Internet access. Wherever possible, alternative forms of access to information and services available on the Internet should be available by other means for clients without Internet access.

Computer Kiosks

Computer kiosks are another method an election management body (EMB) can use to reach voters. Computer kiosks are typically video display screens placed in public locations, such as shopping centres, government information centres or tourist facilities. Any citizen can use a publicly displayed computer kiosk.

Users can usually access information and services through a computer kiosk by using a so called touch-screen or by using a screen and touching buttons on a key pad. Computer kiosk displays, in general, function like an interactive multimedia web site and they can include recorded audio, text, still pictures, moving video and animation.

Computer kiosks can deliver a vast amount of information, in much the same way as an Internet web site, although they are usually not connected to the Internet. Computer kiosks provided by government agencies often include information related to many different areas of government, in which the electoral process is included. Although it is feasible to have a computer kiosk dedicated to the electoral process, it may help to spread the considerable set up and maintenance costs involved in computer kiosks.

By including a key pad in a computer kiosk application, it may be possible to include some interactive services, such as filling up forms and/or paying bills and paying fines using credit cards or other available banking facilities. They can also be used for checking whether personal information and address stored in the voters' register, for instance, is up-to-date.

Desktop Publishing

Desktop publishing is another technology that can be used by election management bodies (EMBs) to reach voters.

Using specialised computer software, it is possible to combine text, numerical data, photographs, charts and other visual graphic elements to produce attractive publication-ready information material.

Depending on the complexity of the material to be produced, an EMB can use a staff member or an outside consultant to prepare it.

In general, a desktop publishing project entails writing and editing text as well as creating graphics and converting photographs and/or drawings into digital images to be inserted in the text. Formatting functions available on desktop publishing software are usually similar to the ones available on word processing software.

Materials produced with desktop publishing technology can include training manuals, voter information booklets and newsletters. This material, complete with artwork and graphics, can be created on the screen exactly as it will appear in print and transmitted directly for production to the printers using a CD or the Internet.

Desktop publishing technology can enable an EMB to produce a relatively attractive and cheap voter information publication in a relatively short time, if needed.

Special Needs Groups

Technology can be used by election management bodies (EMBs) to reach voters in special needs groups. Such special needs groups include people with physical disabilities or mental disabilities, people from culturally and linguistically diverse backgrounds, people in remote areas and people with poor literacy skills.

Audio visual applications

Radio, television, audio and video tapes, as well as some of the more specialised communication devices used by language services, hearing assistance and visual assistance, can be used to reach voters with special needs. In particular, methods that use audio and/or visual recordings meet many of the needs of people who have difficulty reading or understanding printed material.

Some of these technologies, particularly audio tapes and video tapes, may be used to directly target special needs groups.

Language interpretation and translation services

Technology can also be used to communicate with voters in a wide variety of different languages. While several software packages exist that can automatically translate material into a variety of languages, EMBs need to exercise extreme caution if they opt to use these programs because the output needs extended correction, editing and proof reading. The relative complexity and specialized nature of electoral communication can often add to the translation difficulty, but it is very important to ensure that the messages are communicated correctly.

Electoral material in a range of languages can be made available in printed media, in audio visual form, through an automated phone service and electronically on a web site or directly in an electronic voting system. Public broadcast radio in a variety of languages is another effective form of communication, where such services are popular. This ability to reach voters in several languages is particularly useful in a society where significantly large numbers of people speak one or more languages other than the dominant official language.

Automated telephone information systems can also provide information in a range of languages.

Interpreter services in some countries can also be provided by telephone, including three-way conference calls involving the caller, the interpreter, and a person able to answer the inquiry.

An EMB can make use of these telephone interpreter services to complement the telephone information service provided and include the telephone number of the interpreter service with relevant instructions for its use on the EMB public information publication material.

Hearing assistance

Technology can also be used to assist people with hearing disabilities. In addition to personal hearing aid devices, telephones can be fitted with hearing assistance features that amplify sounds for persons using the telephone to access information inquiry lines.

Visual assistance

Technology can be used to assist people with impaired vision. Some countries provide magnification devices in voting places for use by vision impaired people when marking their ballot papers.

An example is the plastic or glass magnifying screen fixed above the writing surface in use at Western Australian State voting sites.

Where electoral information is available to voters on computer screens, the software can be programmed to magnify or zoom in on text and images to make them easier to read by vision impaired people. Similarly, printed material can be created using large point sizes for vision impaired people.

As a general rule, whenever printed material is made available in hardcopy or electronic form, an EMB needs to consider the people who have difficulty reading small print. Adopted fonts and standard point sizes should maximise the number of people able to read them. The same care should also be taken when choosing fonts for printing or displaying text since some fonts are much easier to read than others.
Considerable research has been conducted on font readability, and it is good practice to consult experts in this field when choosing fonts for publications targeting large groups of people, including ones with special needs.

Technology for Voting Operations

Voting operations is understood in this section as the procedures that have to be put in place to ensure that all qualified citizens can exercise their right to vote within established schedules. Different technologies can be used to assist all tasks needed to successfully organize the voting operations.

With the evolution of electoral systems and the increase of the number of voters, most democracies are experiencing pressure to use appropriate technologies as they become available. This is not only to make sure that all voters, regardless of possible disabilities, can exercise their right to vote but also to ensure that election results are known quickly.

At the same time, while some of these technologies have resulted in greater efficiency, they have proven to be controversial since there are opportunities for fraud that might be difficult to trace.

In addition, technology evolves very rapidly, so what is discussed today might be obsolete tomorrow. The ACE project tries to introduce technologies as they appear or at least to provide links to information about new technologies for those who are interested.

The main groups of voting operation technologies refer to:

- logistics of voting operations

- recording votes
- counting votes
- consolidating results regionally and nationally

It is also necessary to take into account that the different technologies adopted for voting operations can have an impact on voting arrangements, on planning of the voting procedures, on acquisition, storage, transportation and distribution of materials and equipment, logistics of the operations and the staffing and training of the polling workers.

In addition, any technology can fail, but in the case of voting operations the impact on the democratic process can be considerable, depending on the level of mistrust among the stakeholders and the political groups. The failure of a voting machine can be considered in a country as a malfunctioning, but in another country it can be suspected as an act of sabotage or even fraud.

As an election management body (EMB) considers appropriate technology for voting operations, it has to evaluate the technology itself and how it guarantees that every vote is counted. It also needs to scan the socio-political environment to ensure that the technology can indeed contribute to the implementation of a free, fair and transparent democratic process.

Voting Operation Steps

Voting operations procedures usually depend on the electoral system and therefore on the relevant legal and regulatory framework, but there are steps common to all voting operations, namely:

- procurement of equipment and supplies needed for allowing voters to cast their vote during the established voting period
- storage of voting equipment and supplies
- transportation of all voting supplies to final destination
- recruitment and management of polling officers
- identification of voting places and publication of

respective list

- voter identification and authentication
- recording of votes cast
- vote counting
- publication of election results
- These steps can use specific technologies, such as:
- procurement systems to facilitate and control procurement of equipment and supplies to be used in the voting boots
- inventory systems to control the storage of voting equipment and supplies
- logistic systems to assist the planning of the transportation of all voting supplies to final destination
- database systems to store and manage information related to polling officers and the voters' lists
- GIS and database systems to facilitate the identification of voting places and respective listing
- voting systems for identification and authentication of voters
- voting systems using optical scanning or direct electronic recording to record and count the votes
- communications systems to support telephone, fax, computer and printers networks.

While considering technology for voting operations it is useful to keep in mind these different technologies, which may be in use already for other electoral administration tasks. Since several independent software systems can run in the same computer, most of these systems can share computer hardware. The same is true for the software, since it is possible to develop different applications to run under the same basic software. For instance

- The GIS software and hardware used for boundary delimitation can also be used to identify polling stations and print the respective lists, although these two applications would run under different and independent programs.

- Database management systems software and hardware used to store voters information and produce the voters' list can also be used to manage electoral administration human resources.
- Procurement systems software used to manage voting operations procurement can also manage all EMB procurement.

Machines used for the voting itself, on the other hand, are too specific to serve other purposes, but some sharing can be envisaged between districts and even between countries with similar voting requirements.

Technology for Voting

The objective of voting is to allow voters to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to choose their government and political representatives. Technology is being used more and more as a tool to assist voters to cast their votes. To allow the exercise of this right, almost all voting systems around the world include the following steps:

- voter identification and authentication
- voting and recording of votes cast
- vote counting
- publication of election results

Technology for voter identification and authentication

Voter identification is required during two phases of the electoral process: first for voter registration in order to establish the right to vote and afterwards, at voting time, to allow a citizen to exercise their right to vote by verifying if the person satisfies all the requirements needed to vote (authentication).

In most countries this process of voter authentication and verification of identity is done manually, but some countries have implemented and others are experimenting with an automated or at least semi-automated method to verify the identity of voters and their right to vote. This implies the existence of an electronic voter register. In fact, the technologies used for voter identification at election time depend on the technologies used to establish the voter register.

Most recent voter identification technologies need to use digitalized voter information and may include the use of:

- smart cards that record a person’s personal information and even biometric data
- database management systems where the digitalized data is stored and managed
- biometric information, such as finger print identification

Smart cards

Smart card technology permits the storage of digital information that can be updated and accessed with an inexpensive reading device that may or may not be linked to a computer network. The smart card, itself, is a plastic card that resembles a credit card and contains a small chip, which includes memory and sometimes a microprocessor. Gold contacts connect the smart card to the reading device. Since it can store more data than a magnetic strip, a smart card can keep the voter’s relevant data, including biometric data, and can also store non permanent data, such as the polling station where the voter is supposed to vote, for instance. Encryption techniques secure the data, and the tiny processor, if it is there, allows the smart card to be programmed for different applications.

Data Base Management Systems

This technology enables the recording, storage and management of required voter data.

Finger printing recognition

While this technology is not new, the electronic methods of recording and recognizing an individual finger print advanced substantially during the last decade of the 20th century. Today, identification can be achieved in a few seconds with reasonable accuracy. As a result, the use of automated fingerprint identification systems (AFIS) that record, store, search, match and identify finger prints is rapidly expanding. AFIS can be integrated in a suite of applications that work together to provide a comprehensive fingerprint and palm print identification system.

Technology for voting and recording of votes cast

Once the voter’s right to vote has been established, the person proceeds to the voting itself. Any credible and reliable voting procedure needs to ensure the voter’s anonymity translated on a secret ballot and freedom of choice meaning that the voter is free of undue pressures. Votes have to be correctly recorded to make certain that every vote counts without being modified.

Through the centuries, different technologies have been used to ensure that a vote is recorded correctly and that it can be accurately counted afterwards. Manual systems using stones, marbles, and paper ballots led to mechanical voting machines and punch cards to achieve faster vote counting. Now electronic voting machines and Internet voting promise more accuracy and convenience.

Voters trust in the voting method is probably the most important consideration in choosing a voting system. In some countries, ballot papers are the most trusted voting method, while others prefer mechanical or electronic machines. Although most countries distrust Internet voting, others are quickly moving to adopt it.

Some countries, especially so called “old democracies”, where voting is not compulsory and that have seen a significant decline in voter’s participation in elections, are aggressively experimenting, with electronic voting machines and with allowing voters to vote using the Internet, usually within a longer period of time.

In the United Sates, mechanical voting machines and punch card systems, which were widely used all over the country to record votes, are being replaced by optical scanning devices and direct electronic recording devices (DRE).

Technology for vote counting

Over the years there has been an increase in pressure to get election results, or at least provisional results, within hours of the closing of the official voting period. This has led to an effort to improve voting systems efficiency and capacity to deliver election results in a short time while ensuring the secrecy of the vote and the accuracy of vote counting.

Many people around the world believe that printed paper ballots (some in Braille for the blind), no matter what the short comings, are still the most accurate way of voting and are the most reliable for vote counting. Others believe that the use of technology protects against fraud and is more accurate and reliable for vote tabulation. In an effort to respond to the pressures of delivering election results in a short period of time, Electoral Management Bodies (EMBs) all over the world seem to be following the technology trend.

Technologies used for voting and vote counting are closely related since most voting machines, besides recording a person's vote, usually have some mechanism, either mechanical or electronic, to count the votes cast into the machine.

The most serious problem with the use of voting machines that count votes can be the lack of a log or paper trail, which could enable a reliable recount in the case of machine failures, suspicion of fraud during vote counting or any other problem. Many vendors of voting systems worldwide are trying to address this problem by providing some kind of paper trail or other trail mechanism to ensure that a vote recount can be done and that election stakeholders can audit both the vote recording and the vote counting at any time during or after the voting session.

Technology for vote tabulation

While vote counting at the lowest level can be manual, tabulation is usually done through a computer or a computer network that may even use basic software such as a spreadsheet, although sometimes a database management system or a custom made program is used.

These vote counting programmes need to be closely scrutinized by software experts to ensure that no fraud is introduced via counting software, which actually can deviate votes to a specific candidate. Programmes with a few lines of code are less likely to introduce vicious code then more complex ones], where it becomes easier to hide fraudulent code.

Another issue is data entry errors, which affects election results. There is a need to have a mechanism to help check data entry error. Usually two different people enter the same data in a computer network and then these two independent versions of the same data are compared: if they do not match, the data is rejected; the error verified against the manual values and re-entered.

This is a tedious process that can be simplified if the vote is recorded in a way that it can be automatically counted. This makes the case for the use of voting machines.

There are several ways to get the vote counted by the voting machine to the next level of vote tabulation, which can be a vote counting regional centre or the local, regional or national election authorities. In some countries, the voting machines are connected to a central computer system through a secure local, regional or national network where all the votes can be automatically tabulated at local, regional and national level.

Mechanical Voting Systems

Mechanical voting systems can take many forms. This includes the use of stones in ancient Greece and the use of marbles in The Gambia It also includes—now considered "old technology" —mechanical voting machines that were once used extensively in the United States and, to a lesser degree, in a small number of other countries around the world. The advent of these mechanical voting machines], when they first appeared, resulted in faster and relatively accurate vote counting.

Mechanical voting/tabulation systems

Mechanical lever voting machines were used for the first time in a United States election in Lockport, New York in 1892, and known at the time as the "Myers Automatic Booth". By the 1960s they were used by more than half of the U.S. voting population. In the 1996 US Presidential election they were used by 20.7% of voters.

These voting machines are no longer built and therefore they have been gradually phased out of use. No mechanical voting machines are expected to be operating in the United Sates by the end of 2006.

On a typical mechanical lever voting machines, the name of each candidate or ballot issue choice is assigned a particular lever in a rectangular array of levers on the front of the machine. A set of printed strips visible to the voters identifies the lever assignment for each candidate and issue choice. The levers are horizontal in their unvoted positions.

Upon entering the voting compartment, the voter pulls a handle that activates the machine and closes a privacy curtain. The voter then pulls down selected levers to indicate choices. The machines are designed to prevent the voter from voting for more choices than are permitted. When the voter has finished voting and exits the voting booth by opening the privacy curtain with the handle, the levers are automatically reset to the original horizontal position for the next voter.
Once voting is completed and the levers are reset to zero, it causes a connected counter wheel within the machine to turn one-tenth of a full rotation corresponding to “one” vote. This counter wheel similarly drives a "tens" counter wheel that in turn drives a "hundreds" counter allowing for counting of up to one thousand votes. The counters are supposed to be set to zero prior to being sent to the voting sites, and this is verified by election inspectors and polling officers.

At the close of the voting period, if all mechanical connections were fully operational, the position of each counter indicates the number of votes cast on the lever that drives it and the counters are supposed to remain locked until final results of the election are published or for a period set by the respective electoral code. Polling officers and sometimes an electoral inspector are supposed to take note of the status of the counters and communicate the results to the local electoral authorities in charge of tabulating the votes. In general, party representatives and electoral observers are also allowed to take note of the votes counted by the machines.

Electronic Voting Systems

Electronic voting or e-voting is a way to get the people=s vote electronically. There are different kinds of electronic voting systems used in several countries around the world. Most of these systems adapt existent technologies or develop specific technologies to be used for electoral purposes.

The main types of electronic voting systems include:

- Punch card voting/tabulation systems
- Optical scanning systems
- Direct recording electronic systems (DRE)
- Internet

Electronic voting systems have been in use since the 1960s, with the introduction n the market of the punch card systems, followed much later by the optical scanning systems, the DRE and the Internet.

Electronic voting machines are used on a large scale in Belgium, Brazil, India, Venezuela and the United States among others. Although there is a trend for adopting this technology there are still many countries that prefer hand-marked and manually counted paper ballots.

While the efficiency of some of these electronic systems is not disputed they have suffered from different degrees of security problems as well as a perception that they are not reliable and that they can introduce substantial counting errors. One of its main advantages though, it is that facilitates voting access to persons with disabilities.

Punch Cards

With punch card systems, voters punch holes in cards using a supplied punch device, to indicate votes for their chosen candidates. After voting, the voter may feed the card directly into a computer vote tabulating device at the polling place, or the voter may place the card in a ballot box, which is later transported to a central location for tabulation.

Two common types of punch cards used in the United States are the "Votomatic" card and the "Datavote" card. With the Votomatic card, the locations at which holes may be punched to indicate votes are each assigned numbers. The number of the hole is the only information printed on the card. The list of candidates and directions for punching the holes are printed in a separate booklet. With the Datavote card, the name of the candidate is printed on the ballot next to the location of the hole to be punched.

Punch cards and computer tally machines were first used in the U.S. for the 1964 Presidential primary election in two counties in the State of Georgia.

Although many U.S. punch card systems are being replaced by more advanced systems, many voters still use them. Punch card systems were used by 37.3% of voters in the U.S. 1996 Presidential election.

Optical Scanning Systems

An optical scanning device combines specialized computer hardware and software. The hardware devices capture an image and software converts the image to computer-readable data.

Voters using machine-readable ballots are given a ballot card with the names of candidates printed on it. Next to each candidate a symbol is printed, such as a rectangle, circle or incomplete arrow. The voter indicates a choice for a candidate by filling in the appropriate rectangle or circle or by completing the arrow.

After voting, the voter may feed the card directly into a computer vote tabulating device at the polling place, or the voter may place the card in a ballot box, which is later transported to a central location for tabulation.

The computer tabulating device identifies the marks made by voters on the cards and records votes accordingly. The individual votes are recorded in a database and aggregated to give total results.

Marksense systems were used by 24.6% of registered voters in the U.S. 1996 Presidential election. Use of these systems in the U.S. is increasing as older lever and punchcard systems are replaced.

There are four main types of optical scanning technologies:

- **Optical Mark Reading (OMR)**
- **Optical Character Recognition (OCR)**
- **Intelligent Character Recognition (ICR)**
- **Imaging technology Optical Mark Reading (OMR) scanning systems**

Most machine readable/optical scanning voting systems use OMR technology. OMR technology has been widely used since the 1970s for a variety of purposes, including school and university tests, censuses, surveys and lotteries, as well as for voting. It is also used in barcode readers, which are in widespread use in retailing, stock taking, libraries and schools.

OMR typically involves a scanner reading particular kinds of marks in a defined set of locations on a page. The computer software used by the OMR scanner is programmed to recognise the meaning of the various marks and to convert scanned images into computer-readable data using the location of those marks.

OMR systems are well suited to first-past-the-post and list electoral systems, where voters are asked to make simple choices when voting, easily represented by a simple mark. In more complex electoral systems, such as alternative voting systems and single transferable vote systems, where voters are asked to choose candidates by showing sequential preferences, it is more difficult to apply OMR technology. As a result, scanning technology has not been used widely for counting these kinds of ballots. However, the increasing accuracy of ICR may make it a viable technology for these kinds of ballots in the 2000s.

Apart from voting systems, there are other potential applications for OMR technology. In Australia, for example, OMR systems are used to scan electoral rolls marked in polling places to indicate the names of electors who have voted. This permits Australian electoral authorities to automate the enforcement of Australia's compulsory voting system, as well as identify any instances of multiple voting.

OMR barcode systems are also used extensively for mailing applications. Many postal authorities place barcodes on mail to automate the delivery process. Some countries have mail systems that allow users to print address barcodes on mail so that postal authorities can process the mail without having to print barcodes in their mail-rooms, thereby creating a discount for the user.

Electoral authorities are also making use of barcodes on mail. Since barcodes can identify both the name and address of the voter, they can be used by electoral authorities to process the mail when it is returned. This is particularly useful for postal ballots to automate the recording of voter names. These barcodes can also be used where addressed mail is returned “not known at this address” in order to capture those details for electoral roll update purposes.

OMR technology is very useful for and efficient at gathering relatively simple, pre-determined data. However, it is not very good at gathering complex, variable data, such as large amounts of text. OCR and ICR systems are more suited to this purpose.

Optical Character Recognition (OCR) scanning systems

OCR scanning systems take scanned images and use computer software to recognise the shapes of printed or handwritten characters such as numbers and letters and store them as computer-readable data. OCR is typically used to convert printed text into computer-readable text.

This capability has many potential applications in the electoral field. For example, in the early 1980s, the Australian Electoral Commission produced an extensive set of procedures manuals. Some years later, when the manuals were due to be revised, the original computer files containing the manuals were not able to be used by the Commission's upgraded computer software. Rather than retype the original manuals, OCR software was used to convert the printed manuals into computer files suitable for editing and revision.

Another important use of OCR is for data capture of information printed on forms. Rather than manually typing information contained on forms, OCR can be used to automatically convert information from forms into computer-readable data.

OCR works by "training" the scanning software to recognise particular shapes as letters and numbers. Since different print fonts are different shapes, OCR systems have to be trained to recognise that a particular letter or number can take several different forms. Given the regularity of printed fonts, this is a relatively straight forward process. OCR systems can also be trained to recognise hand writing. However, given the infinite variety in hand writing styles, this is a much more difficult task.

Early OCR systems had a relatively high error rate when converting printed text to computer-readable data, particularly hand written text. This required a high level of human intervention to proof-read and correct the converted data. As optical scanning hardware and software improved towards the end of the 1990s, the error rates dropped. However, the next generation of scanning systems, ICR systems, went even further in increasing scanning accuracy rates.

Intelligent Character Recognition (ICR) scanning systems

ICR takes OCR systems one step further by using computer software to apply intelligent logic tests to scanned characters so as to more reliably convert them into computer-readable data.

ICR systems apply rules of spelling, grammar and context to scanned text in order to make "intelligent" assessments as to the correct interpretation of the data. This enables much more accurate conversion of scanned text than does the more simple OCR system, particularly with handwriting.

ICR software requires fast, powerful computers to perform efficiently. Reliable ICR systems only became available in the mid to late 1990s with the development of cheap, powerful computer products.

As ICR systems become more reliable, their use for electoral applications will increase. They are particularly suitable for capturing data from forms. ICR systems are also being examined for their suitability to capture hand written numbers from ballots used for more complex electoral systems, such as alternative vote and single transferable vote systems. To date, automatic data capture systems have not been used for these electoral systems owing to the complexity of the task.

Imaging technology

In addition to capturing images for conversion into data, scanners can also capture images to be stored as computer-readable images. Photographs, drawings and images of text can be stored and reused in computer-readable form.

Computerised images have many electoral applications. Images can be included on websites and printed in publications. Staff photographs can be placed on an electoral authority's “Who we are” Internet page and in its Annual Report. Photographs of polling stations can include on websites and instruction manuals. Examples of completed forms can be scanned as images and printed in training manuals.

Paper-based forms can be imaged and stored in electronic form. Copies of the images can then be downloaded over a computer network without the need to access the original paper copies. The Australian Electoral Commission is currently engaged in imaging all of its millions of voter registration forms and placing them on a computer network accessible from any of its offices nationwide. This system will be used to check signatures or any other details included on the forms by accessing the imaged forms on demand.

Corporate logos can be stored electronically as images and printed on a range of corporate publications. Where an organization may once have used expensive pre-printed stationery containing the corporate logo, stationery can now be printed from the desktop with professional letterhead using blank paper, a colour printer and a digitized image of the logo.

Imaging technology can also be used for identity verification purposes. Photographs can be digitized and placed on identity cards. Images of finger prints or facial features can be digitized and stored on smart cards. Software identity systems can be used to compare the image of the person presenting a smart card with the image of the person encoded on the card to determine whether it is the same person.

Direct Recording Electronically (DRE)

The increasing sophistication of computer technology towards the end of the 1990s led to the most recent development in the evolution of voting systems: Direct Recording Electronic (DRE) systems.

Use of DRE systems is expanding and in Belgium, Brasil, India and Venezuela most if not all voters use a DRE device to vote while in the United States and other coutries the percentage of voters using DRE devices to vote is increasing.

Using DRE systems, voters mark their votes directly into an electronic device, using a touch screen, push buttons or a similar device. Where write-in ballots are permissible, an alphabetic keyboard is sometimes provided to allow voters to cast write-in votes.

With DRE systems there is no need for paper ballots. Voting data is stored by the electronic device, on a computer hard disk or a portable diskette, CD-ROM or smartcard. For backup and verification purposes, some systems copy voting data onto more than one storage medium. For example, in Belgium, voting data is written both to a hard disk and to a smartcard issued to the voter. After voting, the voter places the used smartcard in a ballot box. The smartcard can be used as backup should the hard disk copy fail, or as a way of auditing the data recorded on the hard disk.

When the polls close, the data from the various voting locations are amalgamated in a central computer, which calculates the vote totals. Data can be transmitted to the central computer either on removable portable devices such as diskettes, or by a computer network.

Since the 1990s the telephone has also been used as a type of DRE voting system. Voters are able to record votes directly into computer systems using the key pads on their telephones, and to identify themselves with Personal Identity Numbers (PINs), by following a series of recorded instructions.

The introduction of DRE voting options at locations away from polling places, like internet voting and telephone voting, raises the issue of identifying the voter remotely which has not yet been solved to security standards required by the need to ensure that the person voting is indeed a voter, that he can not vote more than once and that the vote is secret.

Internet Voting

The explosion of the Internet and the World Wide Web in the late 1990s led many individuals both inside and outside of the electoral administrations field to speculate about the possibility of using this new public resource to improve the efficiency, effectiveness, and legitimacy of democratic elections. Following on this discussion, several studies and experiments were developed, in independent jurisdictions and with mixed results. The overwhelming consensus which emerged from these studies is that Internet Voting presents numerous risks which need to be properly addressed before widespread deployment can take place.

Why Consider Internet Voting?

The most obvious advantage of internet voting is convenience for the voter. Regardless of how well polling places are designed and distributed, there could be no more convenient place to vote than from the comfort of one's home. By making electoral participation as easy as logging in to a website, checking a few boxes on a form, and clicking the "Vote" button, it is likely that voter turnout, and hence the overall legitimacy of the results, may be improved significantly. It could also allow significant cost-savings in the deployment and operation of physical polling stations, if the "adoption rate" of internet voting is at a sufficient level. The counting and tabulating of electronic ballots is potentially much faster and easier than counting traditional paper-based or even optical-scan or punch-card ballots, which may represent significant cost savings as well.

It is possible to distinguish three different forms of internet voting:

- Polling Site Internet Voting - in which voters cast their ballots via the internet from client machines physically situated in official polling places, in which both the hardware and software of the client is controlled by election officials, and the authentication of the voters may take place by traditional means.
- Kiosk Internet Voting - in which voters cast their ballots via client machines, in which the hardware and software are controlled by election officials, but distributed in public places (shopping malls etc.) in which the physical environment and voter authentication are not directly under official control.
- Remote Internet Voting - in which neither the client machines nor the physical environment are under the control of election officials. Whereas the first two methods are potentially much more secure, they also present few advantages over more traditional voting methods. The "allure" of internet voting is only fully encapsulated in systems in which users are able to authenticate themselves and cast their ballots at their convenience, via home, workplace, or public internet terminals. Unfortunately, it is this method which presents the most serious and intractable security risks.

Security Implications of Remote Internet Voting

The possible benefits of internet voting must be weighed against the risks to which this polling method is exposed. As has been emphasized elsewhere, but bears repeating, every election conducted by whatever means should comply faithfully with the same basic principles of secrecy and anonymity, fairness, accuracy, and transparency.

Every polling system, whether it uses pencil and paper, punch cards, touch-screen (DRE), or any other method, must assure that voters are identified accurately and that their votes are counted accurately. In most cases this must be done without allowing any means to associate a particular vote with a particular voter. It is also essential that the citizenry have confidence in the results; in other words, that the system chosen not only comforms to these basic requirements, but that it does so in a manner that is clear and well understood by all participants. Every polling method should be as secret and anonymous, fair, accurate, and transparent as a well-managed paper-and-pencil balloting system:

> "Indeed, if perfect clerks would conduct an election using paper-ballots, this would provide the best model we have for a public election. Such an election would be, for example: anonymous (avoiding collusion, coercion), secret (all cast votes are unknown until the election ends) and yet correct (all votes are counted) and honest (no one can vote twice or change the vote of another), oftentimes also complete (all voters must either vote or justify absence). In such a system, if we know the voter (e.g., in voter registration) we cannot know the vote and if we know the vote (e.g., in tallying) we cannot know the voter. After an election, all votes and all voters are publicly known – but their connection is both unprovable and unknown."
>
> SafeVote Inc., Voting System Requirements, The Bell, Feb. 2001

Any purely electronic voting system must take into account the necessity of safeguarding the accuracy of the vote count, in the absence of a physical representation of the ballot. For a complete discussion of this issue, see Direct Recording Electronic Systems . In addition to these concerns, Internet voting is subject to other potential risks due to the inherent insecurity of both the user's machine and the network connection by which it connects to the central server or tabulator.

At the present time, over 90% of home computers use a version of the Microsoft Windows operating system. As this operating system was never intended for highly sensitive "mission critical" applications, its primary goal is to be as easy as possible for a novice or casual user to operate. As such, little effort has been made to "compartmentalize" the operating system to prevent "rogue" applications from performing unwanted actions or making unwanted changes to the overall operation and configuration of the computer. This fundamentally insecure environment, along with the widespread deployment of "macro languages" in applications like Word or Outlook, has provided a fertile breeding ground for many different forms of computer viruses, "worms", "spyware", or "trojan horse" applications. Despite the widespread use of firewalls and anti-virus software, it has been estimated that 20% of all personal computers are infected with some type of "malware" (see Your PC May Be Less Secure Than You Think). In other words, there is no way at present for designers of internet voting systems to ensure that the voters' home computers have not been compromised in such a way as to call into question the reliability of the voting process.

Securing the connection between the voter's home computer and the central server is also problematic, but in this area at least the correct use of public-key cryptography allows a degree of confidence in the integrity of this communication channel. Specifically, the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols used by web browsers and servers to create secure channels for e-commerce and internet banking, for example, were designed to prevent the so-called "man in the middle" attack whereby a network transmission is hijacked by an attacker who has managed to control the channel through which the two end-points of the transaction communicate with one another. SSL uses signed encryption keys which have been verified by a trusted "Certificate Authority" to make it impossible for such an attacker to modify the contents of this communication, without revealing that the attack has taken place. Unfortunately, even if this technology is used correctly, it is still vulnerable to other types of attack, which may be characterised as either "denial of service" attacks or "spoofing" attacks. A denial of service attack is said to take place when the attacker, even if unable to alter or interfere with the substance of a communication, is able to prevent the communication from taking place, typically by overloading one or the other endpoint of the communication. A spoofing attack is said to occur when one of the communicating parties is tricked into opening a secure connection to a site controlled by an attacker. A variety of spoofing attack, popularly known as "phishing", has become extremely widespread in recent years, typically involving an email containing an obfuscated link to a site which has been created to perfectly mimic a particular target website (eg. that of a financial institution,) along with an urgent request to "re-enter" sensitive personal information (credit card numbers, passwords, etc.) This is related to a more general form of attack commonly referred to as "social engineering"; that is, bypassing technical security measures by targetting the users of the system, who often have a poor understanding of these security measures. For an informed discussion of the false sense of security created by the widespread deployment of SSL/TLS, see The Maginot Web .

Despite the widespread deployment and use of the internet for banking and other sensitive transactions, it must be emphasised that guaranteeing the security of voting via the internet is a fundamentally more difficult problem, for two important reasons. First, unlike financial transactions, in most constituencies no connection may be made between the voter and his or her vote; record-keeping and auditing capabilities which are standard in the financial world are therefore not applicable to online polling systems. Secondly, discovery of anomolies or errors in the transmission or recording of votes cannot feasibly result in a correction of these results after the fact. At best, such discovery can only result in the invalidation of any votes so affected; at worst, in the invalidation of the election itself. Needless to say such an outcome could have disastrous effects in terms of public confidence in the legitimacy of the entire process.

For a more complete discussion of the security implications of Internet voting in general, see Security Considerations for Remote Electronic Voting over the Internet by Dr. Avi Rubin of Johns Hopkins University.

Real-world Deployment of Internet Voting

The State of Geneva in Switzerland is perhaps the first constituency in the world to deploy internet voting in any widespread fashion. Beginning in 2003 citizens of Geneva have had the option to cast their ballots online. The motivations behind this deployment, as well as the strategies for overcoming the sorts of security issues outlined above, relate at least partly to circumstances particular to Geneva, which may reduce the applicability of this experiment to other constituencies.

Geneva differs significantly from many localities in that citizens are asked to vote much more frequently, typically 4 to 6 times per year rather than once every 2 or more years, as is the norm elsewhere, due to a "direct democracy" system in which any parliamentary vote may be subject to ratification or refusal by the citizenry. As a consequence of this, electoral authorities in Geneva are under greater pressure than their counterparts elsewhere to make the voting process as simple and convenient as possible. In response to this pressure, in 1995 election officials in Geneva implemented a remote voting system based on postal voting, which quickly became the most popular method of voting, and which is credited with increasing voter turnout by 20%. Accepting the viability of postal voting has the effect of "lowering the bar" somewhat in terms of the security and public acceptance issues facing other forms of remote voting; any new system would only need to achieve the same level of security and acceptance as postal voting. For example, registered voters in Geneva already receive voting cards by mail which contains information allowing them to cast their ballots by return post. Internet voting is simply seen as an extension of this well-established service; as such, system designers have simply not addressed potential problems such as vote-buying or coercion by any technical security measures whatsoever, relying instead on socio-cultural norms and legal mechanisms to provide protection against this possibility.

For an overview of Geneva's experiences with internet voting, see the State of Geneva's E-Voting web site ; for a detailed account of security risks and countermeasures considered by the implementors of Geneva's internet voting system, see Addressing the Secure Platform Problem for Remote Internet Voting in Geneva .

Another significant experiment in internet voting, with a more negative outcome, was conducted by the U.S. Military for use by overseas active-duty military personnel. An initial pilot project was conducted during the general election in November 2000 in which a mere 84 military voters participated, despite a cost of 6.2 million dollars, and which was widely considered to have failed to address key security issues. (See Internet Voting Project Cost Pentagon $73,809 Per Vote)

Despite these misgivings, the project was further developed, under the administration of the Federal Voting Assistance Program (FVAP), as the Secure Electronic Registration and Voting Experiment (SERVE), for broader deployment in the general election of November 2004. In advance of this planned deployment, a group of computer security experts produced a detailed study of the system, which concluded that

> "The real barrier to success is not a lack of vision, skill, resources, or dedication; it is the fact that, given the current Internet and PC security technology, and the goal of a secure, all-electronic remote voting system, the FVAP has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough. The SERVE project is thus too far ahead of its time, and should not be reconsidered until there is a much improved security infrastructure to build upon."
>
> A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)

In the aftermath of this report, in February 2004 U.S. Defence Secretary Paul Wolfowitz accounced the cancellation the project, citing these unresolved security issues as the primary reason. (See Pentagon halts Internet voting system)

Conclusions

While it is likely, perhaps even inevitable, that voting via the internet will one day become commonplace, for reasons outlined above it is clear that designers and implementors of internet voting systems face major difficulties which must be overcome before it will be suitable for broad deployment. The most important consideration is the degree to which many crucial elements of any internet voting scheme are completely outside the control of election authorities, with the result that it will be difficult to have any degree of confidence in such voting systems until the architecture of both the personal computer and the internet itself have evolved to a state far beyond that which is currently in place.

Dr. David Jefferson of Lawrence Livermore National Laboratories in Berkeley California, one of the authors of the SERVE Report, has stated that

> "Internet voting systems are vulnerable to denial of service attacks, spoofing attacks, malicious code attacks, spyware attacks, remote management attacks, and automated vote selling schemes. These attacks are powerful enough compromise large numbers of votes, either disenfranchizing voters, spying on their votes, changing their votes, or buying votes. These attacks can often succeed, possibly changing the results of an election, and yet go completely undetected. And they can be launched by anyone in the world, from a disturbed teenager to a foreign government. These vulnerabilities are quite fundamental. They cannot be designed around or fixed with the current generation of PC hardware and software and the current Internet protocols. Until such time as the security architectures of the Internet and the PC have been completely redesigned and the new designs widely deployed, which is probably at least a decade away, Internet voting in public elections must remain out of the question."
>
> David Jefferson, The Inherent Security Vulnerabilities with Internet Voting (Abstract)

And according to American computer security and cryptography expert Bruce Schneier, referring specifically to the American context,

> "Building a secure Internet-based voting system is a very hard problem, harder than all the other computer security problems we've attempted and failed at. I believe that the risks to democracy are too great to attempt it."
>
> Bruce Schneier, Crypto-Gram February 15, 2001

Technology for Corporate Management

Technology can be used to assist corporate management of election management bodies (EMBs). Many of the computer software products available in office automation suites can be used for corporate management purposes.

The types of corporate management processes that can benefit from the application of technology include:

- internal planning processes, such as strategic planning and operational planning
- project management
- personnel management, including recruitment, maintaining staff records, and paying staff
- financial management systems, including estimates

and budgets, expenditure control, financial reporting and audit functions
- supply and inventory management, including procurement, contract management, inventory control, warehousing/distribution control and transport control
- computer systems monitoring and management

The various corporate management systems can ideally be linked together to provide a comprehensive election management system. Planning systems can be linked to project management systems to ensure that projects are in line with the relevant strategic and operational plans. Project management systems in turn impact on the personnel, finance and materials systems. The software systems used for supply and inventory management can be linked to relevant financial management systems to coordinate the estimating, budgeting and payment processes. These systems can in turn be linked to the personnel management system to provide an overarching system that encompasses all aspects of the election management process.

Systems linked in this way should ensure that the election process runs smoothly, with staff properly employed and equipped to perform their functions.

Various software products are available which can assist an EMB with its internal planning processes. Structured software programs can be used to facilitate higher level strategic planning, helping to set goals, aims and visions. Software can also be used for more practical operational planning, which can be more specific and more detailed, including setting tasks and performance indicators.

Software can also be used to enter tasks into calendars, allowing tasks to be scheduled, time lines to be set together with deadlines advance warning and information on meetings an critical dates to be automatically communicated to all relevant staff members.

Project Management

The management of large projects such as the conduct of an election is a complex process, requiring the completion of many tasks and the employment of many people. Recognised project management techniques such as the Program Evaluation and Review Technique (PERT) and the Critical Path Method can assist in ensuring that projects are undertaken successfully.

Powerful off-the-shelf software can be used to assist with the project management process. The software will allow the user to enter tasks to be undertaken, resources needed, critical time lines, and so on. The software can then produce a range of charts, lists and reports which can be used to allocate tasks, estimate costs, monitor budgets, make the best use of available resources and ensure deadlines are identified and met.

Personnel Management

Personnel management is a very complex process that is well suited to computerisation. Software can be used to automate many routine tasks and to store and keep track of the wide range of data needed in a personnel management system. Some of the tasks that such a system can perform include:

- storing data related to each staff member
- storing descriptions of each staff position
- storing pay scales
- assisting with the recruitment process by storing lists of persons who have applied for employment and identifying applicants with suitable skills (particularly where large numbers of casual staff need to be employed for election purposes)
- generating offers of employment and employment contracts
- recording time worked by staff
- calculating payments owed to staff, including salaries, overtime payments, travel and accommodation allowances and other employment awards, and deductions for tax and superannuation
- generating payments to staff, including automatic funds transfers to bank accounts or production of cheques
- generating annual statements of payments and deductions for taxation purposes (known as "group certificates" in some countries)
- calculating leave entitlements and recording leave taken and leave due

While there are many off-the-shelf software programs available to perform these functions, care should be taken to ensure that the program adopted can address the often complex needs of election management bodies (EMBs). In particular, a personnel management program used by an EMB needs to be flexible enough to include employment of a great number of casual staff for election purposes as required. Such a system also needs to allow for any applicable government requirements on payments and deductions related to taxation, retirement contribution and other relevant employment awards, deductions or allowances.

Financial Management Systems

Computerised financial management systems can be used to automate the complex tasks associated with managing the finances of an an election management body (EMB). Such systems can be used for:

- Preparing and calculating estimates of likely income, expenditure, assets and liabilities
- Preparing and monitoring budgets
- Monitoring and controlling expenditure
- Keeping track of invoices and payments, and automating the process of bill paying
- Generating financial reports
- Facilitating auditing of the financial processes

Supply and Inventory Management

Managing the variety and quantity of materials needed by an election management body (EMB) to perform its functions is a large and complex task that is also well suited to computerisation.

Software can be used to identify:

- types of materials needed
- quantities of materials needed
- where materials are stored
- where materials are to be used
- what materials are available and what materials need to be ordered

Software can be used in the procurement process, not only to determine quantities required and time lines for supply but also to assist with contract management. Software can be used to develop tender documents and contracts and to assist with the decision-making process. Software can be used by tender evaluation panels to assess the merits of tenders and to ensure that tenders are evaluated equally.

Software is also particularly useful for inventory control. Where large quantities of material are stored in warehouses or storerooms, it is important to keep track of what materials are stored where. Software systems can perform this task much more effectively than a manual system.

Software can also be used to keep track of distribution control and transport control. This is particularly important where material is dispatched to geographically dispersed locations, such as regional centres or polling places.

The Future of Elections and Technology

The technology developed during the 20th century and first years of the 21st century, particularly computer technology, has in many ways dramatically altered election administration and the way in which elections are conducted. While the basic election tasks of voter registration, voting and vote counting have conceptually remained the same since the beginnings of the modern democratic process, the organization of modern elections, nowadays, depend very much on technology.

It can be expected that new technologies have the potential to continue to change the way in which elections are conducted through the 21st Century.

While it is difficult to identify all changes that future technologies can bring to the organization of elections, some can already be predicted including:

The demise of the paper ballot

Paper ballots have served the election process well. They are relatively easy to produce, easy to mark and easy to count, but they can be quite expensive to print and distribute, they can only be used once, and they are not a particularly good use of resources.

Depending on the type of paper ballots used, they may not be considered the best method to record a vote and can be prone to fraudulent use such vote buying.

Counting paper ballots manually, although relatively reliable can prove to be cumbersome and prone to errors which, in turn can result into the need for multiple counts of the same ballots.

The development of cheap, easily delivered, reusable, reliable electronic voting methods may gradually replace the paper ballot in many countries.

The demise of the polling place

The physical polling place, that has to be rented, staffed and equipped, might become an expensive anachronism in many places where alternative and secure electronic delivery mechanisms can be used. The move to offer government facilities on line, on the internet and in public places may replace the need to organize a physical voting place.

The rise of electronic voting methods

As electronic devices become cheaper, more powerful and more secure, it can be expected that the use of a variety of inexpensive, reliable electronic voting methods accelerates and become more widely used.

Internet voting

While security and identity concerns has lead to caution toward the use of Internet voting, many countries are considering it seriously, for at least some elections, not only to make it easier for the voter but also in an effort to boost voting, since the end of the 20th century witnessed a tendency for voter absenteeism.

It can be expected that not before long these concerns can be answered and Internet voting will become safe, secure and widespread. The potential of the Internet to change the dynamics of both the election process and the wider political process should not be underestimated.

Internet referendums and initiatives

The widespread accessibility of the internet is already leading to the rise of so-called digital democracy, whereby ordinary citizens can vote directly on issues and legislative proposals. Many of these voting exercises are taken as indicative and not binding, but there are already some that are considered binding. In this way voters can be expected to take control of the political process in a manner that was not feasible before. Whether such tendency can turn out to be good for the democratic process is debatable.

Electronic identities

Electronic identity systems are being developed to ensure that citizens can participate in the new electronic world of commerce and government. As more and more daily activities such as paying bills and consulting bank accounts is done electronically, the need to secure reliable electronic identity systems pressure the development and implementation of country-wide and world-wide methods of uniquely identifying people by electronic means.

Electronic information delivery

The 20th century has often been described as the information age. Never before has so much information been readily accessible to ordinary people. It may be expected that the continuing development of the Internet and other electronic technologies leads to an ever increasing availability of information.

This may have a profound impact on the democratic process as the opportunities for information dissemination and retrieval expand beyond the traditional methods dominated by mainstream media. For election management bodies, the emerging electronic information service delivery methods can expand the options available for reaching voters and other clients with a wide range of information products.

Electronic service delivery

In addition to the opportunities of electronic service delivery for the voting process and for the provision of information, many other services provided by election management bodies have the potential to be provided electronically. Voter registration, political party registration, candidate nomination, disclosure of donations and expenditure, provision of expert advice, and other services provided by electoral authorities are already starting to be delivered electronically.

Wireless electronic infrastructure

The current technology uses might be regarded only fit to developed countries, but the first years of the 21st century have already witnessed an important advance on the use of new technologies by countries with weak infrastructures. Notable among all is the opportunities open by the development of wireless electronic infrastructure, delivered by satellite, microwave or radio transmission, which is already enabling electronic service delivery in many remote locations. Combined with cheap, mass-produced electronic registration and voting devices, such wireless electronic delivery systems can be expected to be able to help electronic voting systems to reach any person, anywhere in the world.

Remote service delivery

With electronic service delivery, there is no need for the service provider to be in the same suburb, city or even country as the user. A scenario can be envisaged whereby a local election management body can locate its office anywhere it is convenient for a variety of reasons and its services can be remotely delivered via Internet, wireless and satellite communications or by whatever new technology are invented to replace current technologies.

It really is a brave new electoral world.

Annex

Bibliography

Australian Electoral Commission. *Electronic Voting and Electronic*

Counting of Votes: A Status Report , 2001. http://www.aec.gov.au/_content/what/voting/electronic_report/index.htm

Caltech/MIT Voting Technology Project. *Voting: What it is; What Could be*

Comer, Douglas E. *Computer Networks*. Prentice Hall 2003.

Comer, Douglas E. *Hands-On Networking with Internet Technologies*. Prentice Hall, 2003.

Kurose, James F. *Computer Networking : A Top-Down Approach Featuring the Internet*. Addison Wesley, 2004.

Geneva State Council, Switzerland, *Geneva Internet Voting Project* : http://www.geneve.ch/chancellerie/E-Government/e-voting.html

Germany, Julie A. Barko and Kathie Legg, eds. *Politics-to-go: A Handbook on Using Mobile Tech to Empower Just-in-Time Politics*. Washington: Institute for Politics, Democracy & the Internet, Graduate School of Political Management, George Washington University, 2005. www.ipdi.org.

Mercuri, Rebecca. *Encyclopedic Elections Technology* website. http://mainline.brynmawr.edu/~rmercuri/notable/evote.html , or http://www.notablesoftware.com/evote.html

Ministry of the Interior and Kingdom Relations, the Netherlands. *The Remote E-Voting Project* . http://www.minbzk.nl/

Norris, Pippa. "E-Voting as the magic Ballot? The impact of Internet voting on turnout in European Parliamentary elections" (2002). http://ksghome.harvard.edu/~.pnorris.shorenstein.ksg/ACROBAT/Magic%20Ballot.pdf.

Peterson, Larry L. *Computer Networks : A Systems Approach*. Morgan Kaufmann, 2003.

Stallings, William. *Data and Computer Communications*. Prentice Hall, 2003.

Tanenbaum, Andrew S. *Computer Networks*. Prentice Hall PTR, 2002.

UK Electoral Commission. *The Implementation of Electronic Voting in the UK*. http://www.electoralcommission.gov.uk/about-us/e-votingimplement.cfm.

University of Queensland, Australia, School of Electrical Engineering. http://www.itee.uq.edu.au/~comp3500/A3webs/t1b1/past.htm

US National Commission on Federal Election Reform. *To assure Pride and Confidence in the Electoral Process* . 2001

US Nacional Science Foundation *Report on the National Workshop on Internet Voting*. 2001

Contributors

The ACE Elections and Technology topic area was one of three new topic areas developed after the original nine topic areas were launched on the website in 1998. (The other new areas were Media and Elections, and Election Integrity).

After the launch it quickly became clear to the project team that the use of technology for election purposes impacts so many aspects of electoral administration that it warranted its own topic area. Unlike the other topic areas, which focus on specific areas related to the organisation of elections, such as Electoral Systems, Parties and Candidates, Voter Education and Boundary Delimitation, the Elections and Technology topic area cuts across all facets of the electoral process.

In 2000, Therese Laanela, Project Manager of the ACE project for International IDEA (Institute for Democracy and Electoral Assistance), became coordinator of the Elections and Technology topic area. She assigned the job of lead writer to Phil Green, the Australian Capital Territory (ACT) Electoral Commissioner who had contributed to the Vote Counting topic area.

Phil has been the ACT Electoral Commissioner since 1994, a position he still occupies at the time of writing in 2006. Prior to this, he worked for the Australian Electoral Commission from 1982-1992. The ACT Electoral Commission was established in 1994 to conduct elections for the ACT Legislative Assembly, the local parliament for Australia’s national capital. With the advantage of starting a new election management body (EMB), Phil was able to become an early adopter of technology for election purposes, using computers to automate many election tasks.

When Phil began work on the Elections and Technology topic area, he was involved with introducing an electronic voting and counting system for ACT Legislative Assembly elections. This system (see www.elections.act.gov.au/Elecvote.html) was subsequently used with great success at the 2001 and 2004 Legislative Assembly elections. The ACT electronic voting system remains the only electronic voting system in use for parliamentary elections in Australia (as of March 2006).

Phil took the view that the topic area should be drafted from an election management perspective, rather than a technical viewpoint. While there were plenty of technical instruction manuals out there, there was no lay person’s guide to applying technology to elections. After some initial guidance from Therese and others on the ACE project team, Phil started writing, taking leave without pay from his job as ACT Electoral Commissioner over several months.

The first version of the Elections and Technology topic area went live on the ACE website in 2001 with case studies provided by contributors from around the world, including Palestine, Russia, St. Lucia and the US. Given the nature of technology, the content was almost immediately out of date due to the emergence of new software, new hardware and new experiments in voting technology. The 2001 US election focused the world's attention on "hanging chads" from voting punch cards, and led to calls for "voter verified paper trails" for electronic voting systems.

Aware that the elections and technology topic area would require regular updating to keep it current and relevant, the ACE project team requested that Maria Helena Alves, a founding member of the ACE project and its Project Manager for the UN Department of Economic and Social Affairs until the end of 2002, take on the task.

Helena had built a career as a software systems engineer in private industry until joining the UN New York Computer Centre in 1981. In 1990, she joined the UN Department of Technical Co-operation and Development (UNDTCD) where she worked as an advisor on Information Technology (IT) systems for public sector agencies in developing countries. In 1992, she became involved in the organisation of elections and since then she has designed and managed several UN/UNDP technical assistance projects. She has also participated in numerous technical assistance missions to assess Electoral Commission needs and to assist with specific technical issues.

Providing technical assistance to EMBs in charge of organising elections made Helena aware that more widely available information on issues related to electoral administration was needed. She was invited in 1995 by Horacio Boneo, the first director for electoral assistance of the newly founded International IDEA, to participate in a brainstorming session with experts from all over the world on how to create and implement a globally accessible information resource on administration and cost of elections.

Helena embraced the pilot project produced by the meeting and continued to work on the project to define the technical approach and content requirements for the ACE Electronic Publication, even after retiring from the UN. She coordinated the preparation of the Boundary Delimitation, Election Integrity, Legal Framework, and Voting Operation topic areas for the ACE Project versions 0 and 1.

Helena is proud of what the ACE project has achieved and has cherished working with a great group of people from the member organizations. She says that the experience has been one of the most rewarding of her professional life.

Helena also shares the view with Phil and the other ACE project team members that the Elections and Technology topic area is best approached from an election management perspective. References to more technical oriented sources are made throughout the topic area to assist technicians’ specific needs.

Elections and Technology Case Studies

An Electoral Register from Scratch: The Palestinian Elections of 20 January 1996

Russia - The State Automated Elections System

Saint Lucia

The Use of GIS Software for Redistricting in the U.S. during the 1990s

2014 Indonesian Elections, Case Study :Uploading millions of C1 result forms and achieving a crowdsourced outcome

An Electoral Register from Scratch: The Palestinian Elections of 20 January 1996

An Electoral Register from Scratch: The Palestinian Elections of 20 January 1996

Following the signing of the 1993 Declaration of Principles between the Palestinians and Israel in Oslo, planning started towards the holding of elections for the President and Legislative Council in the Occupied Palestinian Territory: the West Bank, the Gaza Strip and East Jerusalem. The realisation of the Declaration of Principles required further detailed negotiation and agreement: many of the issues related to the elections were included in these negotiations, which lasted until September 1995 when the Israeli-Palestinian Interim Agreement was signed. The political timetable then dictated that the elections should take place as soon as possible: 20 January 1996 was the date chosen. The European Commission signed an agreement with the Palestinian National Authority (PNA) to provide funding and technical assistance for the elections.

No elections of any kind had taken place in the Gaza Strip since the 1940s, and none were held in the West Bank since elections in some major cities in the 1970s. Israeli occupation was withdrawn from the Gaza Strip and Jericho in May 1994 and from some major West Bank urban centres in late 1995, but continued elsewhere. The new PNA had no registration information or infrastructure of any kind. The electoral registration system had to be devised from scratch.

The system was created under a variety of constraints and difficulties:

- The PNA had initially no money and no tax base. Accordingly, major activities such as elections required the agreement of an external donor for financial support, with the attendant criteria and approval procedures.

- The institutions of the Palestinian government were all newly formed and interinstitutional arrangements did not therefore exist. An agreement had to be reached between the Palestinian Commission for Local Government and Elections (PCLGE), the Palestinian Central Bureau of Statistics (PCBS) and the Ministry of Local Government relating to the acquisition of the system for the elections, the assembly of the register and the future use of the system for both electoral and general population/statistical purposes. Tensions existed in particular between the speed and focus needed to create the register required for a fast election and the more extensive work necessary to establish a general population register.

- In addition, while donor support could fund electoral preparations consistent with a wider purpose, the spending of donor funds on activities that contributed only to the wider population register objectives was not allowed under the funding agreements.

- There was considerable debate between PCLGE, PCBS, the Ministry of Local Government, and other parts of the PNA as to which body would have which responsibilities in both the short and long-term.

- The election provisions of the Interim Agreement included requirements for comparison between the Palestinian draft register and the Israeli population register for the Occupied Territories. This strongly influenced the choice of computer hardware and software, in order to ensure that these comparisons were technically possible. A RISC system that used Unix and Oracle was chosen.

- The PCLGE chose an electoral system based on majoritarian voting in 16 constituencies. The register had to be compatible with this system.

Creating the register

The polling hours and the voting procedure were determined by the PCLGE at an early stage, leading to a target maximum of 750 electors per polling station. From their existing estimates of the average household size in the West Bank and Gaza, PCBS calculated a figure for the maximum number of houses per polling district. PCBS then undertook the Community Survey for Elections, which gathered demographic information and which generated hand-drawn maps indicating all buildings within each town, village and hamlet (no other maps being available). The maps were used to define residential polling districts with boundaries that were clear on the ground, each of which was allocated a five digit code consisting of two digits identifying the constituency and three digits identifying the polling district within the constituency.

Qualified electors were required to be Palestinian as defined in the election law, 18 or older on the day of election, and not disqualified for reason of criminal offense or mental incapacity. In order to maximize registration and as part of the process of civic education leading to first elections, the registration in each polling district was conducted through active canvassing by a five member Polling Station Commission (PSC), who were later also responsible for the poll and the count. At least three visits were made to each house to ensure all potential electors were contacted. A registration form for each elector was completed and signed by the elector. In addition, the elector was given a Confirmation of Provisional Registration.

The central computer centre for the registration was established at and run by PCBS on behalf of PCLGE and the Palestinian Central Election Commission, the successor body to PCLGE which assumed responsibility for the election process after the passage of the election law. Each PSC transferred the information from the registration forms on a weekly basis to computer input forms which were designed for both Optical Mark Reader (OMR) and manual use.

The use of OMR machines was an experiment. Although it had been hoped that the bulk of input would take place through the three OMR machines installed, the speed of input in practice was lower than expected. The computer centre was also equipped with 48 manual input terminals designed both for the processing of additions and amendments and as a backup system to the OMR equipment. These terminals were operated on three full shifts over the period of initial register entry, about five weeks, and the task was completed against the very tight deadlines. The importance of a backup system when using what was at that time still developing technology was strongly demonstrated. At the same time, what was a disappointment also gave valuable experience for the possible use of future development of the technology.

During the first five weeks of input, about 1 million entries were made, each consisting of constituency and polling district identifier, name (up to four components), address, date of birth, sex, ID number (nine digits), and ID type (single digit code). In the two weeks before polling day, a provisional register of electors was printed and published on the two heavy duty dot matrix printers installed. As a result of the short time available and the state of the art of technology at the time, this printed register contained only the numeric details (polling district details, sequential elector registration number within the polling district, date of birth, sex, ID number and ID type). The Arabic alphabetic characters—the names and addresses—were written in by hand by the PSC before the publication of the register.

Over the remaining three weeks up to polling, some 30,000 additions and amendments resulting from the submission of claims and objections to the provisional register were input. The final pre-publication draft register was compared with the Israeli population register as contained in the negotiated agreement, and entries that did not match were resolved between Palestinians and Israelis. The final register for the election was then printed, dispatched to PSCs for the hand entry of alpha characters. It was available in all 1700 or so polling districts on the day—only 10 weeks after the first day of the registration canvass.

The purchasing process

The purchasing of equipment for the implementation of the computerised register was funded by European Commission (EC) money and was therefore subject to the EC's procedural requirements. The description that follows reflects the way in which these procedures worked in this particular instance. While the underlying principles of transparency and financial accountability are still of the essence, it should not be assumed that the detailed requirements of this process would now remain the same.

Step 1: Initial budget

A series of contracts were drawn up and signed by the European Commission and the Palestinian Commission for Local Government and Elections (PCLGE), governing the provision of funding for different aspects of election planning and working within the overall budget allocation for support to the elections approved by the appropriate committee of EC member states. Budget lines for the purchase of computer equipment were included in one such contract, based on outline costings established by the EC with PCLGE and the Palestinian Central Bureau of Statistics (PCBS) as part of the initial detailed planning of the EC election support.

Step 2: Tender list

General EC tender requirements provided that suppliers should be drawn from companies registered either in the Palestinian territories or within EC member states. In view of the constraints and difficulties that pertained at the time to supply of goods and customs clearance to the Palestinian territories through Israel, EC approval was obtained to draw up a restricted tender list of companies based within the Palestinian territories. From their knowledge of local computer suppliers, PCLGE and PCBS drew up a list of nine potential suppliers for the equipment and submitted it to the EC for approval.

Step 3: Proposal document

The Proposal Document was drawn up by PCBS and dispatched to the companies on the restricted tender list, giving the companies three weeks to respond. This document contained the technical requirements of the system to be purchased.

The technical specifications included:

- general requirements of the minimum configuration for hardware, including the requirement of full ability to function using Arabic characters, and specifying that any future expansion should not require major changes to the system and therefore that top-of-range models would not be acceptable;
- central processing unit specifications, including expandability, number of terminals supported, and minimum and benchmark performance speeds;
- main memory requirements;
- hard disk requirements;
- magnetic tape streaming unit specifications;
- display console requirements;
- optional terminal server specifications;

- workstation and PC specifications;
- modem specifications;
- Specifications for two heavy duty laser printers, two ordinary printers, a dot matrix printer and two system printers;
- uninterrupted Power Supply (UPS) requirements;
- system communications requirements and diagram;
- UNIX operating system requirements;
- supply and installation requirements of Oracle 7 database management system; and
- the requirement for the tender to define site specifications necessary for the equipment to be supplied.

The detailed specifications offered were to be entered on Technical Data Sheets supplied.

The tenders were also required:

- to specify earliest and latest delivery dates, as time was of the essence in the planning of the election timetable;
- to supply two original complete sets of manuals, in English and also if available in Arabic, for all hardware and software that they proposed to supply; and
- to supply all necessary training and to specify their proposals for this.

Tenders were to be accompanied by a Bid Bond of 5% of the value of the tender, a Performance Bond of 10% of the value of the tender and a Warranty Period Bond of 10% of the value of the tender. The Performance Bond would be retained until the final payment of the purchase price had been made. The Warranty Period Bond would be retained until the warranty period on each piece of equipment supplied had expired.

Payment was to be made in three instalments; 25% within 15 days of signature, 50% within 90 days of delivery, installation and commissioning as evidenced by a Document of Acceptance, and the final 25% only after the complete system had operated satisfactorily for two successive months. The Performance and Warranty Period Bonds would remain in force through this period, and the Warranty Period Bond also afterwards.

Step 4: Evaluation

The interinstitutional agreement between PCLGE, PCBS and the Ministry of Local Government provided for a Joint Procurement Committee (JPC), with three members from PCBS, two from PCLGE and one appointed by the EC. Before opening the replies to the tender, the JPC developed a set of standard evaluation criteria for all bids, scoring 50 points for the hardware and software offered (broken down between all the different items to be supplied), 12 points for the experience and support offered by the company, 18 points for provisions for delivery timetable, installation, documentation and training. The decision was taken to adopt the best technical solution offered as long as it met the criteria of the tender document and the price was within the agreed budget. It was also decided that following further technical consideration after the issue of the tender, the purchase of Oracle would be better made directly from an Oracle agent, and the element of each tender (including the price) relating to the supply of Oracle was therefore ignored.

Tenders were received from all nine short listed companies: two companies submitted two options each, making a total of eleven bids to be evaluated. The tenders were opened and initiated. Six of the eleven tenders were eliminated as not complying with the technical specifications issued.

There were several points of clarification required in relation to the remaining five tenders. A clarification form was accordingly issued in relation to each of the five apparently compliant tenders, with a one week deadline for its return. Following return of these forms, the JPC undertook the evaluation, scored each item of each tender, and placed the five tenders in order.

The negotiation of the final contract between the PNA and the successful tender followed. Minor amendments were made to the originally published payment schedule. More detailed provisions for regular preventative maintenance (to take place every two weeks), 24 hour emergency maintenance cover, the availability without cost of replacement equipment should the equipment supplied fail for more than 24 hours, and the guarantee provisions were agreed.

Step 5: Supply and installation

The contract was signed with the successful tender on 26 August 1995. While there were the inevitable small problems, the success of the system is probably best measured by the fact that electoral registration started on 12 November 1995, with the first registration forms arriving at the newly commissioned election computer at PCBS in the few days following: and that a register of over one million names was completed, printed, reviewed, amended and made available for use on polling day only ten weeks later on 20 January 1996.

Russia - The State Automated Elections System

The Central Electoral Commission of The Russian Federation

Introduction

In Russia, recent advances in democratization have created the need for a new approach to elections. Thus the Central Electoral Commission of The Russian Federation is seeking a modern approach to the running and organizing of elections.

The country's unique conditions, such as its huge territory, large number of time zones, uneven distribution of population,and various regions with differing levels of infrastructure and transport development have all influenced the search for a solution to the organization of elections.

There are at present 105 million voters in Russia. More than 90,000 voting centres are set up during elections, and over one million people take part in the organization and conducting of elections. As a result, the electoral commission faces many organizational and technological problems associated with the preparation and conduct of transparent democratic elections, as well as large financial costs. Of major importance is the preparation of voters lists, running the pre-electoral campaigns, processing and distributing the election results, and insuring transparency of elections. Complications which are unavoidable without the use of modern technology would lead to serious political and economic consequences.

The decree by the President of the Russian Federation to establish a State Automated System Elections was issued on August 23, 1994. From this date an intense development of new Russian election technologies and stage-by-stage implementation of a new electronic system has taken place. The first components of the System were used during the elections of deputies to the Russian State Duma on December 17, 1995.

In June 1996, during experimental exploitation of its first stage, the System was used to prepare and conduct the Presidential elections for more than 80 percent of the subjects of the Russian Federation. The System was used primarily to prepare voters lists and summarize the preliminary results of voting. However, it was effective during this period.

During the elections for heads of executive branches of power, deputies of legislative bodies, and local administrations (October-December 1996), the System was used in 75 (out of 89 total) subjects of the Russian Federation. The operational experience of the System in the subjects of the Russian Federation confirmed its efficiency, comprehensibility and adaptability for solving *local specific problems*, when new software products had been developed with consideration for specific local conditions and local legislation..

The State Programme of the Development of the State Automated System Elections took place from 1996 to 2000. At the time of writing, it was already implemented in 88 subjects of the Russian Federation, i.e. almost the total Russian territory. The scale of its usage and number of technical equipment and technological solutions rank it as the largest computer network in the country. From the point of view of its functional potential, software, and universal structural composition, it is considered the leading information and telecommunication system in Russia.

Possibilities and resources of the System

More than 6000 computers have been configured to form a single system. Out of these, 90 local networks have been created which, in turn, unify more than 300 automated workstations.

The System can provide verification of ballot validity, protect voting results from fraud, and display election results in all regions of the country in real-time mode. On the day of elections, the use of scanners allows the tallying of results of different types of voting with a delay of only 20-25 minutes.Then the intermediate results of voting can be transferred to the Central Electoral Commission as statistics, schemes, text, audio and visual information and, after processing, be promptly forwarded to the media.

In order to provide a high level of sustainability and versatility, various auxiliary components were built into the system. These auxiliary technologies and equipment compose a long list, ranging from various kinds of complex internal furnishing for voting places and centres, to technologies for high-quality printing production with a high level of fraud protection, electronic fingerprint identification devices (dactyloscopy) and ballot-counting equipment.

Between elections these resources are used primarily for:

- communication between administrations at different levels and support for their work
- provision of information resources to administrations

Principles and characteristics of composition, maintenance

The System Elections has a multi-level hierarchical structure, in which automated equipment is linked via email into a single information network. Utilization of different communication channels (including digital and satellite channels) allows the System to operate in a real-time mode.

The first cycle of the System serves as a technical basis for computer networks at the four major levels: Central Electoral Commission, Electoral Commission of the Subjects of the Russian Federation, District Electoral Commission, and Regional Electoral Commission (see scheme 1).

The hierarchical structure of the System duplicates the organizational structure of Electoral Commissions:

- information network of the Central Electoral Commission and the Informatisation Federal Centre;
- information centres of Electoral Commissions of subjects of the Russian Federation;
- information services of District Electoral Commissions conducting elections of the federal bodies of state power;
- information centres of Regional Electoral Commissions.

Although local networks at lower levels have unified software and telecommunication bases, their characteristics and configuration differ from each other. For example, primary (low-level) networks for the Regional Electoral Commissions can be manufactured in six different models differing from each other in their terminal characteristics and number of printers, depending on the intensity of information flow and the number of voters in a region.

The Systems composition is based on the module principle, which allows the development of the System, without affecting the operation of its basic networks. This principle also allows the use of components of the network autonomously in certain areas for conducting different kinds of elections and serving other local needs.

Today, the System Elections is one of the largest information systems in Russia and provides reliable and sustainable *electronic communication* with the most distant regions of the country. It provides email services for more than 3000 clients in almost all cities and regional centres of the Russian Federation.

The System is operated and maintained by more than 3000 system administrators. Technical maintenance is supervised by 25 internationally certified technical consultants, who have permission from the government to work with the System. Twelve regional service centres provide training of personnel and maintenance of technical equipment.

The second cycle of the System Elections will include modernization and automatization of the Divisional Electoral Commissions. As a result of this work, the total number of local networks and terminals integrated into the System will reach 100,000 units. It is anticipated that the System "Elections" will be unified with other information systems in Russia, which are currently being developed through various federal development programmes.

Technical solutions

The communication system and data transformation project was developed in accordance with the current state of the Russian communication channels, using foreign and domestic technologies and equipment, and taking into consideration the specific administrative and territorial composition of the country, local geography, and a relatively low level of computer literacy among the population.

Major criteria for selecting technical and computer hardware were a high level of reliability during the exploitation period and the universality of its composition.

The local network is composed according to the Ethernet 802.3 and 802.12 technologies, which will also facilitate local video conferences. In addition, eight file-servers and three email servers are used. Standard Compaq computers, ProLiant and ProSignia servers, and DeskPro and ProLinea workstations were used as components of the System.

Using telecommunication channels, information about voting is collected in the Central Electoral Commission, thereafter it is processed by "Itogi" (Results) and Kartographia (Cartography) programming tools, and subsequently sent to the Elections Information Centre.

The Elections Information Centre uses the system of information display for prompt distribution of information about the process of elections and voting results.

The information display system is a combination of software and hardware unified into a local computing network. One of the elements of the system is a Toshiba videowall—a screen four metres in diagonal. The information display system allows the protection of a picture covering the whole screen, as well as different pictures only covering parts of the screen. Depending on specific tasks, it is possible to display information in poly-screen mode, i.e. to display information on a single segment of the screen or on four, nine or sixteen segments or to combine two pictures.

Data is transferred to the information display system through digital communication channels. This kind of hardware support provides maximum flexibility and dependability of the system with minimal supervising personnel. Transfer of sound, pictures and data in "video-conference" mode complies with the ISO Ethernet standards.

Technologies of data collection and processing

From the beginning of the voting procedure until the signing of final protocol by the Central Electoral Commission, the System Elections is used for monitoring the election process and receiving preliminary voting results by transferring data from subordinate Electoral Commissions to superior ones. The technology for data collection from subordinate Electoral Commissions includes:

- *Data collection of the election process*. Information about the election process is collected at Regional Electoral Commissions, processed by Electoral Commissions and transferred to the Central Electoral Commission. This information includes data about the number of voters registered in voting centres on the day of elections, overall number of voters voting at a particular moment, dynamics of the election process, and percentage of voters who have already voted.
- *Provision of operative information about the voting process*. Information is collected and processed by the Regional Electoral Commission and transferred to the Central Electoral Commission. It includes voting results from all Divisional Electoral Commissions, which have presented reports.
- *Provision of preliminary information about the voting process*. Information is collected and processed by Regional Electoral Commissions, after collecting final protocols with voting results from Divisional Electoral Commissions. After processing data from all Regional Electoral Commissions, Electoral Commissions transfer it to the Central Electoral Commission. This data represents voting results from Regional and District Electoral Commissions.
- *Establishing archive databases.* Archives are compiled from databases created in Regional Electoral Commissions and Electoral Commissions during the

> election process. Information received by the Central Electoral Commission network from subordinate Electoral Commissions is double-checked in order to eliminate all possible mistakes and is stored in respective databases.

Programme Complex Itogi (Results) allows information to be summed up and presented as tables, including subjects of the Russian Federation, Regional and District Electoral Commissions, and the percentage of processed bulletins compared with overall numbers.

Programme Complex Kartographia (Cartography) presents election results on in [CONFUSING] cartographic forms using colours, graphics and diagrams. After each session of data processing, slide series are produced. Using communication channels, tables and cartographic information are later transferred to the information display system.

High quality technology was used during the election of the President of the Russian Federation and the elections for the state authority bodies in 1996, when the State Automated System "Elections" was used for summarizing preliminary voting results.

System of communication and data transfer

A digital automated station and leased communication channels are used at the upper level of the System. They provide reliable voice communication and data transfer (19,2 Kb/sec) using "each-to-each" principle, and compose the departmental communication network of the Central Electoral Commission.

Introduction of new communication equipment and digital communication channels will speed up the data transfer up to 64 Kb. Implementation of a wide-line telephone and communication system with moving objects is also planned. At present, a half-duplex mode for data transfer and a duplex mode for telephone communication are used.

Direct telephone, facsimile, modem and teleconference communications are used by the upper level of the System for communicating with the Electoral Commissions. The System can interact with other networks, and is able to use additional number capacities of the Moscow City Telephone Network, non-state Russian networks Rosnet, Rospak and others.

During preparation and conduct of federal elections, all available channels of communication are used for data transfer, ranging from commuted telephone channels (switch-boards) to apportioned digital and satellite channels. Commuted telephone channels and regional and/or other local networks of data transfer are used at the lower level.

Data (information) protection

Information in the System is protected from unauthorized access by means of organizational and technical/software.

One of the Systems administrators in each section of the System has additional responsibilities for data protection. The System's administrators have software and hardware capabilities for data/information protection in each section. A routine for data/information protection from unauthorized access provides:

- data/information protection from unauthorized access during data processing;
- a register of access of authorized network users to information, software and hardware resources;
- controls for keeping the resources for System safeguards and software programs intact;
- registration and accumulation of all data about breaches in operation of the System relating to its security;
- control of workstation users' activity and prompt use of safeguard measures.

Software

The System software is composed of general and special software, which allows automated data collection, processing and analysis on all levels of the System.

General Software of the System Elections is composed of software for usual operation. General Software includes:

- Russian information/telecommunication package used in the telecommunication equipment. Using a transport module, it provides data reception and transfer via e-mail in auto mode on all levels of the System.
- **Novell Netware and Windows NT** used in network operation systems.
- **MS Dos and MS Windows** used in the basic operation environment.
- **Paradox for Windows and Clipper** used in database management systems.

Special Software of the System Elections is a package of multi-functional programs developed in Russia. It provides solutions for a complexity of tasks of the System during elections, summarizing the voting results as well as being used between elections.
The package consists of the following major software:

- **VOTER** —including voter registration, preparation and printing of voters' lists.
- **TERRITORY** —including classification and location of territories, residential communities, and Electoral Commissions.
- **RESULTS**—providing updated information about voter participation during the voting procedure, processing of preliminary information about voting results, and preparation of materials for publication.
- **CANDIDATE/DEPUTY** —this includes maintenance of lists and files of candidates, proxies, electoral organizations and blocs which nominated candidates, deputies, and preparation and registration of deputies' certificates.
- **FINANCES** —for planning, fulfillment and control of budgets of Electoral Commissions, and accounting.
- **LAW**—maintains normative, legislative and regulatory documents in electronic version.
- **SECRETARY**—provides capability to work with documents (incoming/outgoing, regulatory, registered in electoral body), control over distribution, and completion of documents and instructions.
- **STATISTICS**—allows processing and analysis of statistical data on voting results, graphic and cartographic representation, and interaction with other networks for obtaining statistical data.
- **CARTOGRAPHICS** —provides prompt cartographic representation of information about preparation, conduct and results of electoral campaigns.
- **PLANNING**—facilitates complex automatization of the work of Electoral Commissions during planning and preparation of events, and conduct of elections and referenda.

Scanners for voting bulletins

Scanners for voting bulletins is an optical electronic peripheral device for scanning and processing ballots in voting centres. They were first introduced and broadly used during the elections in the Russian Federation in 1996. During the election of the President in June 1996, scanners were used in 15 Moscow voting centres for the preliminary processing of ballots.

During the election of the Governor of St. Petersburg in the same year, the number of scanners used reached 60. For the elections to bodies of local self-governance of 600 Leningradskaya oblast and 10 in Saratov. It is expected that scanners will be one of the most important election technologies used in Russia.

They allow the automation of the following operations:

- scanning votes marked on voting bulletins;
- counting votes for candidates and votes against all candidates with accumulating results;
- registration of results on magnetic storage diskettes and paper;
- checking correspondence of bulletins to approved specimens to prove validity;
- identification and automated marking of invalid ballots or ballots not corresponding to approved specimen.

Utilization of special software in scanners allows for effective usage according to local conditions, especially in remote regions.

Saint Lucia

Infrastructure considerations

Saint Lucia has good microwave, satellite, cable, television and Internet connections.

Equipment in unprotected areas can be subject to undesirable effects from heat, humidity and rust (because most large communities are near the sea and Saint Lucia lies in a hurricane-prone zone).

Main power is generally reliable in supply but subject to major fluctuations. For this reason voltage regulators protect the equipment. The IBM AS/400 mainframe computer is attached to an uninterrupted power source (UPS) with a one-hour electrical backup time, supported by two generators on a dedicated electrical circuit.

The PCs, dumb terminals and printers are maintained in-house but AS/400 repairs are supported from the neighbouring island of Barbados. The systems are all developed and maintained in-house. Except for back-ups, very little operator intervention is required. The infrastructure required to support and maintain our current and proposed equipment and systems is therefore quite good.

Technology acquisition

The decision to acquire our current equipment was made by a Steering Committee of four set up for that purpose. This Committee was given clear terms of reference and a three month deadline to produce reports on tenders received and a recommendation on the preferred equipment. Three possible suppliers were invited to tender and after extensive demonstrations and questioning one was recommended.

The choice of the IBM AS/400 system was determined by a number of factors:

a) It was clearly the most advanced mainframe of the three, since it was the only one whose architecture was specifically designed to support a relational database.

b) It was the only machine whose combination of vertical and horizontal machine interfaces ensured that it would not become obsolete for a very long time. That is, these interfaces render the underlying hardware of the AS/400 transparent to the user.

c) The operating system (OS/400) is sufficiently complex to obviate the need for Systems Programmers or highly trained operators.

d) The logical layout of the OS and the programming tools supplied made it easier to concentrate on WHAT to do rather than HOW to do it.

e) The system has excellent and easily implemented security features at various levels—from physical workstation location down through object and field levels.

f) The system compels object-oriented programming.

g) Many large organisations (such as General Motors, Citibank, etc.) have spent huge amounts of money to switch to this system and even Microsoft uses it to run its business.

Saint Lucia is forced to purchase their own hardware because there are no bureau services within the country. For security reasons, this would have been the case even if there where any bureau services. A policy of developing software in-house was adopted because this meant that trained people with a thorough understanding of the systems would easily be available. Also, this meant that it was possible to get an exact fit for the needs at that time and to maintain that fit as the requirements change. The transfer of technology this entails, as opposed to the "no-brainer" of merely running a package was also a factor in this decision.

The communications systems are direct twin-ax cabling and leased lines. The direct cabling is a feature of the specific machine and leased lines, rather than dial-up, were chosen for security and availability considerations. PCs are used for Internets, email, etc., and an IBM product, Client Access, is used to connect PC Local Area Networks to the AS/400 via direct twin axial cabling.

Minimizing the risks in using technology

The mainframe is housed in a special computer room within the computer centre. There are numbered keypads for access to both the computer centre and the computer room within it. These codes are regularly changed. A security guard is also posted at the entrance to the building. Physical security of workstations located at user sites other than in the computer centre is the responsibility of the various users.

Access to data is limited in several ways:

a) All classes of users can only sign in at their specific physical locations.

b) Passwords are required for all users and the system forces password changes on a regular (though variable) basis.

c) Upon signing-on, users get menus enabling them to perform certain tasks and some tasks are restricted to certain users. Users may not exit these menus.

d) All major objects (files, data areas, programs, etc.) on the system are accessed according to the users specific level of authorization to each object. These levels are read only, read/write, update and delete. While data entry and validation are on-line, all master file updates are run in batch after a log of the additions, changes (before and after images) and deletions has been produced for scrutiny by a supervisor.

e) Each individual command or program call indirectly issued by each user is monitored in that users job log.

The software code is contained in files and is secured in much way the same way as data. The AS/400 does not lend itself to infection by viruses, and all PC used in our Local Area Networks are protected by North and Macaffee anti/virus software. The reliability of registration data is clearly crucial. This data is mainly collected from birth certificates and certification by Justices of the Peace in the area in which the potential voter resides.

From time to time voter location checks are carried out and the names of voters who cannot be located are published in the press. This system is fairly reliable but the absence of a direct link with the Registry of Births and Deaths is a major existing deficiency. There is clearly a need for some sort of permanent identification number that will follow each person from birth to death. This number should not be meaningless (as the voter registration number now is) but should be based on date-of-birth, sex and any other relevant factors. Apart from its usefulness for voter registration maintenance, this number can be used throughout Saint Lucia for National Insurance, Drivers Licences, etc.

The SAVCHGOBJ (save changed objects) command is used to perform daily backups of all changed objects in the system. This is done on a grandfather, father, and son basis. In other words, one set of tapes are used to backup changed objects on Monday, a second (different) set on Tuesday and yet a third set on Wednesday. The Monday tapes are used again on Thursday and so on. In addition, monthly saves of the entire system are carried out. The system is not available if the AS/400 is down but, since this machine is so reliable (it has only been down once in nine years), this is not a major concern. However, it may be useful to create a simple data entry system on a PC to allow unvalidated data entry to proceed if the system is down. This data can then be uploaded and validated in batch when the system comes back up. There are plans to implement mirroring on the new AS/400 Model 170. The RAID (Redundant Arrays of Inexpensive Disks) technology used by this model clearly lends itself to this approach.

The AS/400 hardware has its own diagnostics that warn of hardware problems both predicted and actual. It also provides the ANZPRB (Analyze Problem) procedure, which greatly facilitates dealing with any problems that may arise. This procedure takes a user step-by step through the process of identifying the problems, ascertaining their probable cause and taking the steps required to correct them. In addition, the System Arbiter, in combination with the Performance Tools package, continuously tunes the system by dynamically allocating storage, maximum activity, wait states, job time slice, etc. The problems that have arisen in the past have almost always been with third-party peripherals but the core system has been exceptionally reliable—even though it is never shut down.

Monitoring of and reporting on system communications is automatic. Because of the basically non-numeric nature of electoral data, only simple totals and changes to these totals can be directly tested by computer staff. The users carry out more comprehensive testing on a random basis.

The hardware is insured but there is no insurance against contingency loss.

The various political parties, and indeed the public at large, appear quite comfortable with the level of accuracy of the voters lists so public assurance measures are not an issue at the moment. All the information currently held in the Voter Registration System is essentially in the public domain, so the issue of privacy does not arise.

Using technology for voter registration

The Voter Registration System is used for recording eligibility for voting, prevention of impersonation, and planning for polling. The voter registration qualifications are uniform throughout the state. All voters must be registered and must be in possession of a Voter

ID card. This is a laminated card carrying the following information: name; date of birth; nationality; address; sex; height; voter registration number; national insurance number; date of birth; date of registration; distinguishing marks (if any); and a colour photograph of the voter.

The Electoral Commission fixes a cut-off date for registration before each election. The information on the card (except the photo) is entered into the electoral register kept on a central AS/400 computer. Certain other information not appearing on the card is also collected and entered including occupation, constituency and polling district.

The computer system allows authorized persons to enter, change and delete information from the electoral register but keeps a record of the date and time of any changes and the user profile name of the person involved. The system produces lists of voters in alphabetical order within a polling district in the constituency. A similar list in registration number order is also produced. From time to time the electoral office carries out an ID confirmation exercise and publishes lists of people who are on the electoral register but cannot be located by the enumerators for their district. These people then have ninety days to present themselves to the enumerator to confirm their existence. Failing this, they are deleted from the register. Deletion does not involve the actual removal of the voter record from the computer system but merely means that the record is marked as deleted.

On Election Day, the voter registration lists are used by the polling clerks and the agents representing the various candidates, in conjunction with the ID cards, to determine voter eligibility. The ID cards, while required, do not by themselves necessarily confer the right to vote.

United States

Although many countries are considering the adoption of Geographic Information Sytems (GIS) software for redistricting, and a few are very close to being able to use this software in an upcoming round of redistricting (Australia and Canada, for example, are well on their way to developing GIS capabilities for redistribution purposes), very few countries to date have actually used GIS software specifically for redistricting. New Zealand is an example of one country that employed GIS software for their last redistribution in 1998. The country with the longest experience using GIS software for redistricting purposes, however, is the United States.

Although the number of states in the United States that were employing computers for redistricting purposes had been steadily growing since 1970, two important changes led to the dramatic increase in the number of states that used computers for redistricting during the 1990s:

- the diffusion of affordable GIS software
- the introduction of a new computer database by the U.S. Census Bureau in 1990

Prior to 1990, most states used a low-tech approach to redistricting: staff and legislators, in stocking feet, used grease pencils to mark proposed district lines on acetate overlays over large census maps spread out on the floor. Adding machines or handheld calculators were used to aggregate the population counts of the census areas that were being combined to create proposed districts. If computers were used at all, they were used as giant adding machines.

By the 1990s round of redistricting, however, every state in the United States used computers for redistricting, and almost every state used GIS software for redistricting. The major reasons for this shift was the increasing availability of GIS software, some explicitly designed for redistricting purposes, and the advent of a computerised map base of the entire nation by the U.S. Census Bureau.

In the United States, the U.S. Census Bureau is required to conduct an enumeration of the population every ten years and to supply the states with this population data for redistricting purposes. States, as well as local entities such as counties and cities, are required to redraw legislative lines on the basis of this data prior to the first election after the census.

The redistricting data produced by the Census Bureau is referred to as PL 94-171 data. It includes population counts for several different levels of census geography—units as large as whole counties, and units as small as census blocks (usually the equivalent of one city block), are reported in PL 94-171. Although the Census Bureau collects data on a large number of population characteristics, only a few items are included in the data files sent to the states for redistricting. These items are total population, voting age population, and subtotals of the population for persons of Hispanic origin and for five major racial groups: white; black; Asian and Pacific Islander; American Indian, Eskimo, and Aleut; and "other" races. This data has been available in electronic format since the 1980 round of redistricting.

In addition to population counts of the entire country, the Census Bureau also maintained a master set of 26,000 maps of varying sizes and scales of the country. These maps were drawn by hand, and were often difficult to read and filled with errors. In preparation for the 1990 census, however, the Census Bureau created a computerised database of the entire country called TIGER (Topographically Integrated Geographic Encoding and Referencing). The TIGER database depicts visible geographic features such as roads, rivers, and railroads; a whole hierarchy of census geographic units (for example, census blocks, block groups, and census tracts) for the collection and reporting of population data; the boundaries of administrative subdivisions such as counties, cities and towns; and political geography such as congressional districts and, in some cases, voting areas—referred to as election precincts in the United States. Maps produced from the TIGER database provided U.S. redistricters with uniform, digitised maps for the entire country for redistricting purposes in the 1990s.

As the TIGER files became available, GIS software was also increasing in availability. A number of commercial companies offered GIS software that was customised specifically for redistricting purposes. These GIS software packages were able to relate information on population demographics, taken from the census, and political data from previous elections to the computerised TIGER base maps showing geographic census units, election precincts, street networks, natural and built landscapes, other jurisdictions boundaries and other geographic features.

The implications of these new products was overwhelming for those involved in redistricting: affordable GIS software and a consistent nation-wide computerised database that included both census data and digitised maps was available for both those charged with the task of redistricting and for those simply interested in evaluating proposed plans and producing alternative plans.

One of the substantive results of this confluence of events was the active and informed participation of numerous interest groups that had previously been excluded from the redistricting process in the United States. The participation of civil rights groups, in particular, led to the adoption of redistricting plans in many states that gave minority groups much greater representation in the halls of government. For example, 24 new minority congressional —districts in which minority voters made up a majority of the voters—were created and more minorities elected to Congress than ever before. To create these districts within the tight population equality constraints imposed, however, a number of other districting values had to be compromised—in particular, the geographic compactness of these districts.

This case study illustrates some important points to be made about the use of GIS software for redistricting.

- The availability of electronic data and computerised maps makes the adoption of GIS software for redistricting a relatively simple task. Because the U.S. government provided the electronic data and computerised maps for the entire country—and at a very low price—redistricters were able to make use of GIS software without having to be concerned with creating an electronic database.

· Many public interest groups were also able to purchase the electronic data and GIS software because of the affordable price. These groups used the data and software to evaluate proposed redistricting plans and to create alternative plans. This information was used to hold the redistricters accountable and certainly had a democratising influence on the process in many instances. (Clearly, the increase in the number of minority districts drawn during the 1990s round of redistricting is directly attributable to the active monitoring of the process by minority and civil rights groups.)

Although there is potential for GIS software to "democratise" the redistricting process, this is possible only if the boundary authority is truly non-partisan or if all parties and interest groups interested in the redistricting process can gain access to the necessary data and technology. As computers and GIS software become more affordable, this is becoming less of a problem. But in many countries, the necessary hardware and software may still be prohibitively expensive to most groups. In addition, training on the use of GIS may be difficult to acquire.

2014 Indonesian Elections Case Study: Uploading millions of C1 result forms and achieving a crowdsourced outcome

Link to PDF

The credibility and success of an electoral process can hinge on how well an election management body (EMB)tabulates and releases the election results. Results face intense scrutiny from an impatient public eager to learn the outcome of a lengthy election process. Political agents lobby to influence the compilation of results in order to capitalize on every advantage and increase their hold on power. Collecting results from thousands of locations from every corner of the nation is a complicated logistical task demanding the careful coordination of thousands of election staff. This volatile combination of visibility, risk, and complexity creates a situation where any error or misstep in the release of results can derail a peaceful democratic transition of power.

In 2014, Indonesia’s election commission, the Komisi Pemilihan Umum (KPU), faced a renewed challenge to deliver credible and fast election results. In the 2009 presidential election, the KPU was able to provide an acceptable election result thanks, in part, to a fortunate combination of factors: the race featured a clear frontrunner, media coverage agreed on the results, and a set of unanimous and accurate quick counts were published ahead of the official results. The 2014 presidential election featured two candidates representing very different visions for the future of Indonesia who ran a close election with sophisticated campaign strategies aimed to win at all costs. This case study looks at the challenges the KPU faced in delivering the 2014 presidential election result, and how it was able to increase transparency of the result tabulation to inject credibility into the process that was crucial for the success of the 2014 election.

Situation

The election law obliges the KPU to conduct a manual tabulation of the results at every level of administration: polling station, village/ward, sub-district, district/municipality, province, and finally nationwide. Votes are counted at the polling station soon after polls close on Election Day at 1 p.m., generally in daylight and plain sight of the community. Once counted, a copy of the result sheet (C1 form) is posted at the polling station and another copy is carried forward to the village level, where the first step of manual tabulation takes place. Manual tabulation continues through four more administrative levels. This process takes about 30 days to complete legislative elections and somewhat less for the simpler presidential ballot. The complexity of the tabulation process poses risks for interference with data at each level of tabulation, especially in conflict-prone areas or areas where there is a lack of observers and media attention.

In preparation for the 2009 presidential election, the KPU made efforts to produce a quick (and therefore electronic) election result. Due to the short timeline, the KPU accepted support from the Agency for the Assessment and Application of Technology (BPPT) to create a nationwide electronic result system that would scan the paper result forms, read the data off the paper, and tabulate a nationwide election result. In theory, the system was supposed to deliver preliminary results within days. Unfortunately, the system never delivered an election result as the project was besieged by a number of problems, including inadequate testing of the system, minimal staff training, lack of public awareness, procurement problems, and technical equipment malfunctions.

However, in 2009 external circumstances were conducive to ensuring that the result was ultimately accepted by the public. Specifically, three conditions helped establish the credibility of the election result. First, the 2009 election featured a strong incumbent president running for reelection and unanimously favored to win the race by a wide margin in all major opinion polls. Second, on Election Day, media outlets unanimously reported exit polls that reinforced the predictions of the pre-election surveys. Third, quick counts came in throughout the evening that confirmed the results of the exit polls - with 10 agencies predicting the actual result within 1 percent of accuracy. By the end of election night, there was no confusion over who had emerged the winner even without the official results from the KPU. Thirty days later, the KPU released the final result, which confirmed what the nation already understood. The losing ticket challenged the results, but the Constitutional Court swiftly dismissed all charges as there was no doubt about the election outcome.

In the lead up to the 2014 presidential election, public opinion surveys made it clear that it would be a very close contest between the two candidates. As presidential hopefuls polled head to head, every vote would be seen as significant in influencing the outcome of the election. Any mishap in the publication of the election result could be used to cast doubt and bring into question the entire process. In order to ensure the integrity of election result, the KPU soon realized that in addition to processing results through all administrative levels as soon as possible, it needed to ensure the process was transparent and credible.

Solution

Based on its previous success in cooperating with the University of Indonesia’s Computer Science department (Pusilkom) during the voter registration reform and voter list development, the KPU once again partnered with Pusilkom to establish a result publication system that was transparent and proved able to work in a very short timeline.

With less than three months until Election Day, options were limited. Another rushed implementation of a last-minute solution would increase the risks of repeating the failures of 2009. With the advice from experts, the KPU reviewed its options and identified three solutions that had potential to work:

1. For official results: Implement a spreadsheet (Excel) template of the result tabulations at each level of the official and law-bound results process .
2. For transparency and evidence: Scan all result forms from each polling station and publish them online for public verification and evidence in legal challenges.
3. For quick preliminary results: Data entry of the result forms at community offices with preliminary results in 48-72 hours.

With the technical support of the University of Indonesia’s IT team, the KPU pursued all three options with varying degrees of success for the legislative election in April, which in a way served as a pilot test for the presidential election. The KPU published the Excel tabulations on its website from the sub-district, regency, provincial, and national levels as well as the scanned images of the polling station results (C1 form) from about 81 percent of the polling stations. Due to the open list proportional system, the legislative election result was too complex for these technologies to successfully deliver a reliable result and the final, manually tabulated result was delivered by the KPU within the mandated 30 days.

2014 Presidential Election Day

On 9 July 2014, as the nation finished voting in more than 500,000 polling stations, over 135 million ballots were counted in broad daylight, in front of entire voting communities at each of the polling stations. By 5 p.m. that day, based on average samples of 2,000 polling stations, eight quick count companies declared the Jokowi-Kalla ticket as the winner, while three quick count companies called the race for the Prabowo-Hatta ticket. The KPU realized the election may become too close to call and the pressure mounted for publishing the official result as fast as possible, while ensuring accuracy and transparency at all levels of tabulation.

As thousands of tabulation workers from 497 regional KPUs worked tirelessly to tabulate results at the regency (kabupaten/kota) level, they also began scanning C1 forms from each polling station in their regency/municipality. The C1 forms are completed after counting at each polling station and contain information on the number of registered voters, number of people who voted, ballots used, valid votes, and the number of votes gained by each candidate. Within the first week, 98.53 percent of C1 forms have been scanned and uploaded to the KPU’s website (http://pilpres2014.kpu.go.id/c1.php).

The availability of scanned C1 forms inspired a popular movement - Kawal Pemilu - to employ best practices in technology and social networking and create a full election result within days after polling. On 13 July 2014, as the KPU conducted plenary meetings to consolidate votes at village level, a group of developers outside of Indonesia launched a website to follow the recapitulation process. Kawal Pemilu, literally “guarding the election”, built an efficient web application that allowed users to look at the scanned C1 forms and enter the results into a database that then compiled the totals. The Kawal Pemilu team employed sophisticated techniques to ensure the site was quick, reliable, and secure, which in turn enabled the team to produce a fast, credible result. The site was quite a technical achievement for only a few days’ work. Within six days, while the KPU continued to manually consolidated votes at the province level, the website had input 97 percent of the data that had been uploaded by the KPU.

However, Kawal Pemilu was much more than a technical achievement, it was a social phenomenon. Kawal Pemilu organized a strategic crowdsourcing effort to enter the results quickly while also protecting the accuracy of their work. Kawal Pemilu began with a small set of trusted friends compiling results. These volunteers could then invite others to participate and vouch for their reliability. These trusted volunteers would sign in to the system using their Facebook account, which added an additional layer of accountability. In only five days, their worldwide data entry staff grew to 700 members and completed 97 percent of the work.

This trusted network of volunteers, built virtually overnight by leveraging the best of open data principles and social media potential, delivered full election results to the Indonesian public. By 22 July 2014, the KPU released their final results and confirmed the same results of earlier quick counts and the online effort headed by Kawal Pemilu.

Without public support in providing transparency, the KPU would not have achieved a credible election. The election was fierce and Joko Widodo won by a margin of less than 6 percent or 8 million votes over Prabowo. The independently crowdsourced tabulation provided an alternative source of information among divergent quick counts, which minimized the conflict between the loyal supporters of both candidates.

Conclusion

With only months to spare, the KPU was able to put together a results solution that benefited from the lessons learned in 2009 and increased the transparency of the results process just enough to enable a credible election result. The steps the KPU took in 2014 created the most transparent and auditable Indonesian election result to date. The KPU’s success was also supported by outstanding contributions of public participation, such as Kawal Pemilu. Without citizen-driven initiatives, the doubt cast over the election could have lingered just long enough for the result process to be hijacked or the winner to be declared by the courts instead of the votes.

The technological solution to deliver a faster unofficial result worked due to the simplicity of the system. The KPU used scanners and applications compatible with all computers at the regency/municipality level. The system was easily grasped, and one week of training proved sufficient for operators to master the Excel forms that were designed to replicate the paper result forms.

Lessons Learned

- Assistance from national and international experts and academics can create conditions for electoral success. The electoral environment may hamper direct international assistance, but an EMB can still benefit from international experiences and advice. The KPU was able to use expert advice to: establish a feasible results strategy that avoided a repeat of results uncertainty of 2009, establish a technical partnership with the University of Indonesia IT department, and increase the transparency of the results tabulation process just enough for Kawal Pemilu to step in and complete the job on the KPU’s behalf.

- No product an EMB produces captures the public’s attention more than the final results. An EMB cannot treat results as an afterthought simply because they occur late in the electoral timeline.
- Electoral public discourse is sophisticated – enormous capital is employed in manipulating meaning and perception, and campaigns will use every trick in the book in pursuit of victory. An EMB needs quick, accurate information to maintain a clear, credible voice throughout the process and actively contribute to the electoral conversation. The tabulation of the final election results offers the best, though far from the only, example of an EMB’s challenge to remain credible in a turbulent environment.
- Technology must be used in a way that increases transparency in order to increase electoral credibility.Transparency is the most effective anti-fraud measure in tabulating election results.
- Technology must be user-friendly for election commission staff in order to minimize human error during the tabulation process. IT infrastructure conditions, human resources, and the timeline are important considerations in determining appropriate technologies for use in an election.

Elections and Technology

full text on one page

Consolidated Replies discussing Elections and Technology

Consolidated replies are summaries of the discussions on the Practitioners' Network. Below replies related to the topic Elections and Technology. Browse Consolidated Replies on all topics here.

Are you an experienced election practitioner and not yet a member of the ACE Practitioners' Network? Apply and join the network now: www.aceproject.org/apply.

- Online candidate nomination (27 Jul 2016)
- Questionnaire design for assessing challenges of implementing electoral technology (05 Aug 2015)
- Iris Biometric Voter Registration in Somaliland (30 Jul 2015)
- Experiences with Internet Voting (17 Jun 2015)

- Use of drones on election day / Uso de drones el día de la elección (16 Jun 2015)
- Discarding or retiring defunct voters' rolls (06 Jun 2015)
- GIS/GPS Mapping of Polling Stations in Sierra Leone (05 Jun 2015)
- Using Failure Mode Effect Analysis (FMEA) for elections? (15 Sep 2014)
- Biometric Voter Registration and Voter Identification (26 Aug 2014)
- Checking the candidate supporter lists (15 Jul 2014)
- Electronic Election Observation (11 Jun 2014)
- Country experiences with electronic voting (10 Jun 2014)
- Experiences with online testing of election staff (26 Mar 2014)
- Actions undertaken by EMBs to increase voter registration (19 Jul 2013)
- Pros and cons of a permanent computerized electoral list in Benin and its impact on voting operations (18 Apr 2013)
- Consultations on internet voting (27 Mar 2013)
- Scope and functions of the IT Division of an Electoral Management Body (15 Nov 2012)
- Social media and voter education (08 Oct 2012)
- The Swedish 'free right of nomination': Other examples? (06 Jul 2012)
- Biometric Voter Registration: Skills required and problems encountered? (21 Jun 2012)
- Examples of Outsourcing Functions of EMBs (02 May 2012)
- Biometric voter verification in Ghana (12 Mar 2012)
- Age limit for biometric identification (05 Mar 2012)
- Using mobile phones for reporting voting results (25 Jan 2012)
- Paper audit trail in e-voting (09 Nov 2011)
- Electoral districts for greater accountability (31 Mar 2011)
- Serial numbers on ballots (14 Feb 2011)
- EMBs using Automatic Finger Identification Systems (AFIS) (23 May 2007)
- Electronic Voting Machines - Blank vote option (19 Dec 2006)