



Report of the State Comptroller of Israel | May 2025

Cyber Defense

Information Systems and Cyber Protection in Municipal Elections



Information Systems and Cyber Protection in Municipal Elections

Background

Municipal elections represent a fundamental pillar of local democracy, and its results have significant impact on various aspects of daily life for all residents of the State of Israel. In Israel, elections for local authorities and regional councils take place every five years concurrently across the nation. The statutory date for these elections during the audit period was initially set at October 31, 2023. However, due to the onset of the Iron Swords War, the elections were first postponed to January 30, 2024, and subsequently took place on February 27, 2024 (elections actual date). These elections proceeded amidst the war in all local authorities, with the exception of twelve local authorities where residents were evacuated, and in some of those local authorities, elections were held in November 2024.

The election process can be a target for hostile entities attacks, which aim to undermine the sense of security and trust in state institutions, a risk that is exacerbated when elections take place during wartime. Since the commencement of the Iron Sword War, the Israel National Cyber Directorate has reported an increase in the frequency, variety, and targets of cyberattacks within Israel. The total number of significant incidents during the war, from October 7, 2023, until the end of that year, amounted to 3,380, reflecting a 2.5-fold increase compared to routine times. Furthermore, the objective of the majority of these attacks was to inflict damage, in contrast to pre-war incidents where the main goals were espionage and information theft.

The Minister of Interior is responsible by virtue of the law for the local authority election process, ensuring that elections are conducted properly and in compliance with the law, including upholding fundamental principles such as general, direct, equal, confidential and proportional elections. The Senior Local Authority Elections Division within the Ministry of Interior (the Supervisor Unit), headed by the National Supervisor of Elections (the Supervisor), is responsible for managing and supervising the electoral process. With respect to the information systems employed in the electoral process and their cyber aspects, the Supervisor is the entity that delineates system requirements, while the Senior Digital and Information Technologies Division at the Ministry of Interior provides the necessary development and maintenance services.









Although the election process itself is manual – utilizing ballot voting where each voter deposits their ballot into a ballot box – information systems are being used in preparation for and the managing of the elections for several functions, including personnel recruitment and training; task management in preparation for the elections; dissemination of voter eligibility



information; accessibility of election-related information and polling locations; as well as the inputting election results into the computerized systems and publishing the results to the public. Various government ministries develop and maintain some of these systems, adhering to numerous regulatory bodies in the cyber domain. A diagram illustrating the systems involved in the electoral process is provided below.



Information Systems Used in the Local Elections Process

Responsible entity	Name	Description
 The Population and Immigration Authority	System C	Managing information about the candidates and the parties, on those eligible to vote and on the final results
 Ministry of Interior	System B	System for managing the electoral process
 Ministry of Interior	System D	Receipt of the voter register files
 Ministry of Interior	System E	Viewing temporary results
 Ministry of Interior	System F	Official information website for the local elections
 Ministry of Interior	System G	Website for obtaining based information on the location of polling stations on the eligible voter's details
 Ministry of Interior	System H	System for managing requests from candidates and representatives for electoral lists from the voter register files
 Ministry of Interior	System I	Learning system

According to data from the Ministry of Interior, processed by the Office of the State Comptroller.



Key Figures

**NIS 1.26
billion**

The budget for local elections (including its changes) as of January 2025, of which NIS 29.7 million (2.35%) are actual computing expenses

**12,000
polling stations**

Were placed across the country in municipal elections

30,000

The number of workers employed in local elections

**About
500,000**

Operations for entering data from candidate forms and lists that were filled out manually into the computerized information system (involving data entries taking several days and were subject to human error) during the examined elections.

120,000

Votes using outer envelopes, in both rounds of municipal elections, which are checked manually and not digitally

Audit Actions



From July 2023 to July 2024, the Office of the State Comptroller examined of the information systems and cyber protection measures pertinent to municipal elections. The audit was performed at the Ministry of Interior, specifically within the Supervisor Unit and the Senior Department of Digital Technologies and Information. Supplementary examinations were conducted at the Population and Immigration Authority (Population Authority), the Prime Minister's Office (Israel National Cyber Directorate), the Ministry of Justice (Privacy Protection Authority), and the Ministry of Economy and Industry (National Digital Agency).

The audit was also conducted in real time, commencing during the preparatory phase of the election campaign. During the course of the audit, the Office of the State Comptroller submitted certain findings to the auditees to enhance their preparedness for the elections, with some issues rectified prior to election day. On election day, election night, and in the subsequent days, teams from the Office of the State Comptroller performed



an audit of the command-and-control center managed by the Supervisor Unit, the sorting center for outer envelopes, and the intake centers of thirteen local authorities nationwide, all under the jurisdiction of election managers employed by the Supervisor Unit, who received election materials from the polling stations and entered the election results into computerized systems.

The subcommittee of the Knesset State Audit Committee decided not to place on the Knesset's agenda and not to publish particular data in this report for national security reasons, pursuant to section 17(a) of the State Comptroller Law, 1958 [Consolidated Version].

Key Findings



Digitization of the Elections



Promoting Digitization and Automation in Electoral Processes – The cost of the local authority election process in 2024 was NIS 1.26 billion (not including the public holiday) and predominantly remains manual in nature, encompassing two core procedures: voting and the identification of voters, which have potential for computerization. Furthermore, the Supervisor Unit has not automated the manual forms utilized for electoral purposes, including thousands of nomination forms submitted by 737 candidates across 3,643 electoral lists, as well as approximately 11,000 voting minutes. The Supervisor Unit uses basic automated tools for core operations in the electoral process, but those tools are inadequate for executing complex calculations, despite the availability of advanced data analysis tools on the market, such as legally compliant random assignment tools for monitoring the assignment of faction representatives to polling committees. Additionally, the Supervisor Unit continues to rely on manual operations performed by human agents, which are susceptible to errors, such as typographical mistakes, and pose a risk of information leakage during the transport of sensitive materials.

It is noteworthy that in December 2013, the then Minister of Interior established a public committee to examine the computerization of electoral systems for the Knesset and local authorities. The committee's activities were suspended in 2014, and this matter was not promoted by subsequent Ministers of Interior and election supervisors, despite the fact that computerized electoral processes have long been established in the primaries of certain parties in Israel and are implemented in several countries globally, with the exception of a specific initiative in 2023 by the Ministry of Interior to computerize the process of electoral list submission and examination, which is currently awaiting legislative approval.



👎 Lack of Knowledge Sharing and Pooling of Resources Between the Knesset and Local Authority Election Processes – The main processes taking place within the two electoral systems (Knesset and local authority elections), which are budgeted and maintained by two public entities – the Central Elections Committee (responsible for the Knesset elections) and the Ministry of Interior (overseeing local authority elections) – face several professional challenges that are, in part, similar. These processes have been managed and developed over the years, without coordination or knowledge sharing between the entities, nor resource pooling – thus inhibiting the efficient and optimal use of public resources where such efficiency is feasible. Joint initiatives could facilitate mutual learning, thereby improving similar processes, mitigating risks to electoral integrity, improving the efficiency of systems, and preventing redundancy in the development and maintenance of similar information systems. It is noteworthy that both entities are presently engaged in separate endeavors to develop new computerized systems. This collaborative process would further enhance conceptual development and strategic planning regarding digitization and automation within these two electoral systems.

Manual Inspection of Outer Envelopes, Rosh HaAyin, First Round of the Elections




Photographed by teams from the Office of the State Comptroller on February 28, 2024.



The Support by State Regulatory Entities in the Realm of Information Security and Cyber Protection

Regulatory Guidance of the Electoral Process with Regards to Cybersecurity –

There is a lack of an integrating state regulatory body in the realm of information security and cyber protection that provide guidance and support the election process, ensuring that all systems and infrastructures employed meet the requisite level of protection. This absence is notable given the national significance of the project, which profoundly affects the public, society, and the economy, particularly regarding the utilization of information systems where breaches could lead to the disclosure of sensitive data pertaining to millions of citizens, compromise the integrity of system information, disrupt the operational continuity of these systems, and ultimately undermine public trust in state symbols and democracy. Although the Israel National Cyber Directorate and the Government Cyber Defense Unit (YAHAV) have been involved over the years in the development and maintenance of certain systems related to information security, such engagement has been partial and inadequate, failing to provide a comprehensive solution. Under these circumstances, it was not until May 2023 – five months prior to the originally scheduled election date in October 2023 – that the Supervisor Unit within the Ministry of Interior formally reached out to the Israel National Cyber Directorate, asking its assistance in the current electoral process. In reality, only in September 2023, less than two months before the original election date, while the systems were already utilized, definitive arrangements were established between the National Cyber Directorate and the Ministry of Interior, determining the framework for focused support from the Supervisor Unit concerning the computer systems and critical procedures during the 2023 election campaign.


 **Protection of Sensitive Information in the Voter Register –** The voter register contains sensitive information regarding millions of eligible voters. This confidential data is disseminated prior to elections to numerous parties, including hundreds of candidates and thousands of electoral lists. The Privacy Protection Authority issued guidelines only in September 2023 and directed the Supervisor Unit to relay these guidelines to the register's recipients belatedly, over two months after candidates were entitled to receive the voter register. Consequently, the guidelines' relevance was significantly diminished, as by that time the information could have already been misused in a matter not compliant with the regulations. Furthermore, the Authority failed to execute crucial active measures for raising awareness and enforcement among the register's recipients, actions that were undertaken during the Knesset elections. This is especially critical given that elections for local authorities involve a more extensive distribution of voter information to a larger pool of candidates and parties, increasing the associated risks, particularly in an environment marked by a rise in information security incidents during wartime. The Privacy Protection Authority mentioned that those measures were not taken due to resource constraints during the war, as some of its resources were allocated to managing severe information security incidents affecting the economy.




Identification and Management of Cyber Incidents


Utilization of Systems on Election day Without Risks and Threats Analysis –


On election day, the Supervisor Unit utilized additional information systems not included in the systems mapping documentation and in the threats and risks analysis. Consequently, a suitable protective framework for these systems was neither evaluated nor established, and they were not scrutinized in terms of information security and cyber protection aspects pertinent to the elections, nor were they subject to real-time monitoring to detect cyber incidents.

 **Detection of Anomalous Cyber Events –** On election day, the Ministry of Interior did not operate a central Security Operations Center¹ (SOC) for integrating monitoring findings from all supporting election systems, resulting in a lack of an integrating entity having a complete overview and an ability, using computerized means, to discern connections between anomalous events across various systems. Furthermore, the reference threats defined by the Ministry of Interior in collaboration with the Israel National Cyber Directorate were inadequate, lacking comprehensive consideration of all potential threats that could inflict significant harm to the electoral process. Additional deficiencies were identified in additional systems and in monitoring.

 **Handling of Events Suspected as Cyber Incidents –** The Ministry of Interior did not establish a structured process and actions protocol to follow upon identifying an event suspected of being a cyber incident (aside from notification by the SOC division to relevant elements within the Senior Department of Digital Technologies and Information), including essential preventive measures to be enacted immediately upon detection of an attack. The absence of a structured and clear action plan for swift activation upon the identification of an attack may result in prolonged attack durations and exacerbation of damage.

Protection of Sensitive Information

 **Logical Protection –** Deficiencies were identified in the logical protection mechanisms concerning sensitive information within the local authority election process. These deficiencies pertain to issues such as permission management, passwords management, separation of powers, and database protection.

 **Access Control and Safeguarding of Sensitive Material –** In nine (69%) of the 13 authorities observed by representatives of the Office of the State Comptroller on election day, deficiencies in physical access control were noted, permitting unauthorized individuals to access areas where sensitive election materials were stored. Furthermore,

1 SOC – Security Operation Center – a command-and-control center for monitoring, identifying, and responding to cyber events



significant gaps in the physical safeguarding of sensitive election materials were identified, as these materials were often left unattended, thereby posing a risk that could compromise the integrity of the elections.

Sensitive Materials Left Unattended on Election Night in Intake Centers (Merhavim and Petah Tikva, Respectively from Right to Left)



Photographed by the Office of the State Comptroller teams on February 27, 2024.

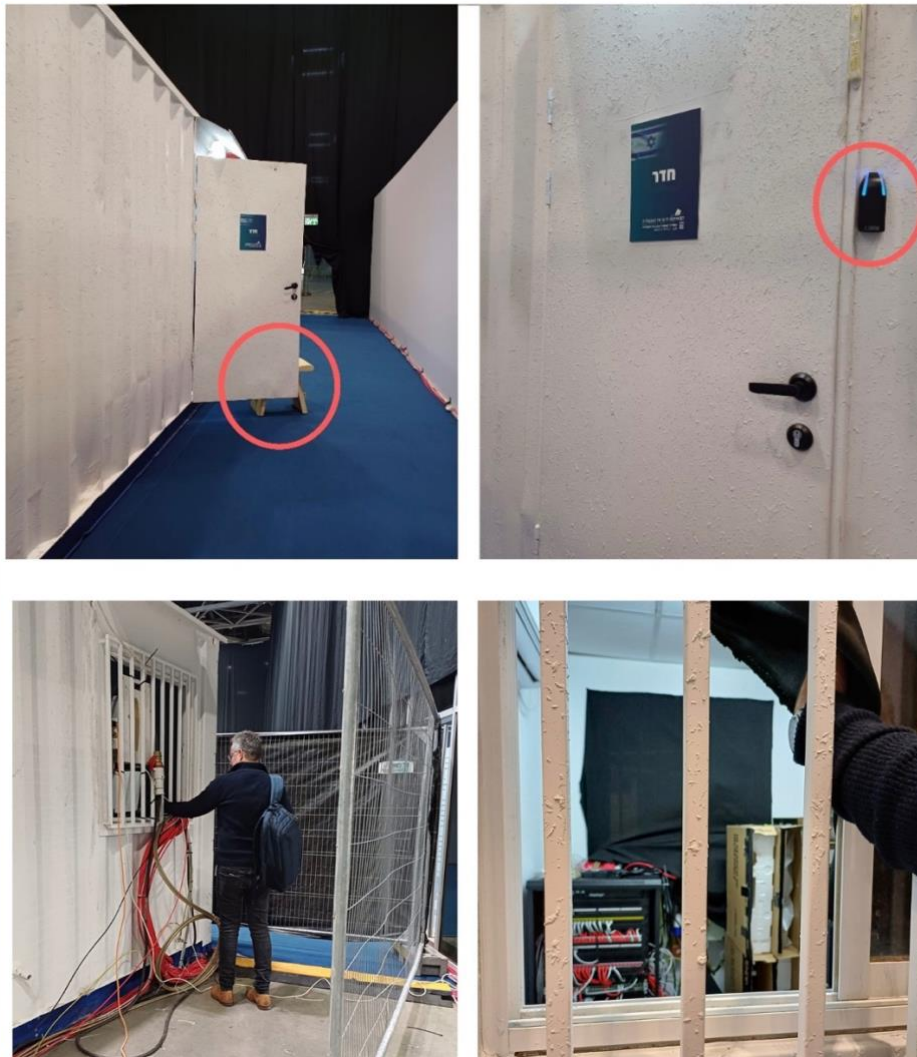
* The photos show sensitive materials that were left unattended, not in accordance with procedures.

System C

User Workstations – On election night and election day, the Population and Immigration Authority deployed numerous remote System C stations with the objective of eliminating candidates and lists from the system and verifying the relevant authority's association with the outer envelope. The stations were placed without implementing requisite physical protections (access prevention and access control), as mandated by the Government Cyber Defense Unit guidelines, and were not compliant with the Population and Immigration Authority's requirements. The disparity between the risk arising from the absence of necessary protections on the stations and the advantages of their placement is further accentuated by the limited utilization of the stations at these locations, with only 0.2% and 8% of the envelopes being examined through them, respectively.



A Room in the Control Center on Election Night




Photographed by the Office of the State Comptroller teams on February 27, 2024.


- * Contrary to the guidelines established by the Population and Immigration Authority, the entrance door to the System C polling station complex remained open for a portion of the time, despite the installation of a card reader intended for access control. Furthermore, the security protocols governing the communications cabinet and the communications cables for the remote stations were found to be inadequate, failing to meet required security standards regarding the structure, cabinet and cable location, and control of access.




Interfaces

-  Deficiencies were identified concerning the interfaces between certain systems.

Systems Development

-  **A New System to Manage the Electoral Process** – The Supervisor Unit and the Senior Department of Digital Technologies and Information at the Ministry of Interior commenced in 2019 the development of a system (A) to manage the election processes scheduled for 2023. This system, for which the estimated cost of the order was approximately NIS 40.9 million, was intended to supersede in the 2023 elections the systems utilized in prior elections and to address deficiencies and challenges inherent in those systems. However, the system's development was not completed in time for the elections, and consequently, approximately eight months prior to the elections, the Ministry of Interior, following recommendations from the Senior Department of Digital Technologies and Information, opted to cease development of System (A) and put into service a previously utilized System (B). The audit found that this decision was made by the Ministry at a juncture that did not afford adequate time for the necessary preparations to utilize System (B) effectively. Thus, for example, the system was deployed without comprehensive testing. Throughout the elections preparation period, various malfunctions were noted, such as inaccessibility and a lack of alignment with user requirements, when on election night, significant issues arose regarding the system's functionality, including the inability to enter voting results due to insufficient authorizations for officials and an undefined list of candidates. As a result, alternative systems (the backup system or the local authorities' system) were utilized, resulting in delays of several hours in the entry and publication of overall results. Additionally, in discussions conducted on election night by teams from the Office of the State Comptroller with 13 election managers, nine (69%) reported experiencing operational challenges with System (B) during both the preparation phase and the election day itself.

-  **Secure Development and the Performance of Penetration Testing in Advance** – The Ministry of Interior and the Population and Immigration Authority did not adhere to security protocols within certain information systems developed and procured for managing the electoral process at local authorities, contrary to the requirements delineated in the Government Cyber Defense Unit guidelines. Moreover, the Ministry of Interior performed penetration tests in proximity to the original election date, and was required system modifications following the identification of vulnerabilities, such as the potential for uploading malicious files. The timing of these penetration tests did not allow sufficient opportunity for the implementation of substantive corrections or compensatory controls that would have been necessary for the proper functioning of the systems had the elections proceeded on their original date of October 31, 2023. However, given the election date postponement, it was feasible to carry out the necessary corrections prior to the new election date.



Managing Systems in a Public Cloud – During the 2024 elections, the Ministry of Interior reinstated² System (B) on a public cloud platform located abroad, following the addition of new developments to the system. This action was undertaken without thorough examination concerning information security and privacy protection aspects, and without obtaining re-approval from a government cloud committee, a procedure mandated by the Government Cyber Defense Unit for any government information system transitioning to a public cloud or undergoing significant modifications, in light of the potential risks associated with utilizing a public cloud platform abroad, particularly regarding information governance. Additionally, System (B) lacked the compensatory controls mandated for System (A) as a prerequisite for its transition to the cloud.



Candidate Data Entry Process – An observation conducted by the Office of the State Comptroller team during the candidate data entry process identified deficiencies. These deficiencies were subsequently reported to the Supervisor Unit and the Population Authority and were addressed in accordance with the team's recommendations

Key Recommendations



It is recommended that the Minister of Interior promote the digitization and automation of election processes with considerable computing potential, including voter identification via biometric methods, computerized voting, automation of nomination forms and protocols for polling station secretaries, the creation of a voter list management system to enhance the handling of outer envelopes (which totaled 114,578 in round one and 7,497 in round two of the current elections), computerized management of the assignment process for polling committee members, and the application of artificial intelligence technologies. The automation of these processes will facilitate the optimization of time and human resources, enable the analysis and processing of extensive databases, enhance information security concerning sensitive materials in the electoral process while decreasing the necessity for their transportation, assist in controlling procedures, increase transparency within the process, and reduce the risks of human error and of compromising the integrity of elections. In promoting digitization, the estimated cost of the local authority election process in 2024, projected at NIS 1.26 billion excluding public holiday costs, will be taken into consideration, as well as the holding of computerized elections in Israel across several non-state entities (such as party primaries) and in various countries including the USA and Estonia, and the decentralized nature of the local authority election process (with each authority operating

² System B was used for the 2018 election campaign. The Ministry of Interior developed a new system for the 2023 elections, but the development was not completed on time and the Ministry decided to use System B for the 2023 elections.



independently), permitting a controlled and gradual transition to digital applications through the implementation of a pilot model. It is also recommended that the Minister of Interior consider initiating legislative modifications on the subject, should they be deemed necessary.



Considering the similarities between local elections and general elections to the Knesset in terms of the business processes and information systems utilized during the preparation and management stages, and acknowledging that the Ministry of Interior and the Central Elections Committee are currently in the planning and initiation phases of new information systems for overseeing election processes, it is recommended that the Minister of Interior, in coordination with the Chairman of the Central Elections Committee, recommence the activity of the Committee for the Computerization of Electoral Systems for the Knesset and Local Authorities, which was ceased in 2014, and collaborate with the Supervisor Unit and the Central Elections Committee to establish a forum that fosters digitization and automation in election processes while facilitating knowledge sharing and resource pooling. This collective effort aims to address challenges by integrating technology into the electoral process while developing mechanisms that encompass aspects of information security and cyber protection.



Given the Ministry of Interior's statutory responsibility for the comprehensive management of the electoral process, which encompasses all facets including cybersecurity, and recognizing the Israel National Cyber Directorate's contribution to supporting the electoral campaign, enhancing protective measures, and engaging all state entities in cybersecurity efforts to safeguard this critical national process, it is recommended that the Ministry of Interior and the National Cyber Directorate take steps to amend the existing regulations. This may include modifications to the Law for Regulating Security in Public Bodies, the Local Authorities (Elections) Law, 1965, or the adoption of alternative legislative frameworks that would mandate ongoing guidance and oversight by the Israel National Cyber Directorate in local authority elections concerning all systems, infrastructures, and bodies engaged in the electoral process. This approach aligns with the recommendations made in the State Comptroller's report regarding the necessity for continuous guidance for general elections. It is important to emphasize that the regulation regarding guidance and supervision does not diminish the Ministry of Interior's overall responsibility for leading and managing the local authority election system. This approach will yield a comprehensive protection framework for all systems and infrastructures integrated into the project (including the interfaces between them), encompassing capabilities for asset mapping, threat reference definition, intelligence gathering, conducting briefings and exercises, and performing penetration tests on all participating entities. Additionally, it is recommended that the Israel National Cyber Directorate remains involved in the development of systems during the interim periods between elections.



It is recommended that the Privacy Protection Authority undertake supplementary actions to the guidelines it has issued concerning the distribution of the voter register in electoral processes, including raising awareness, supervision, and enforcement. It will further ensure that these actions are conducted in advance, especially prior to the availability of the



register for download, thereby enhancing their efficacy and relevance while considering the risks and numerous factors involved in the local election system, extending beyond the national election system.



It is recommended that in forthcoming electoral systems, the Supervisor Unit meticulously map all systems utilized in the electoral process in advance, including the business processes and information managed within each system, the system users, their interfaces, and categorization. This will facilitate the creation of a designated protection framework for these systems aligned with the risks they present, alongside testing to guarantee that these systems adhere to the established protection standards.



It is recommended that, in alignment with the defense doctrine, the Ministry of Interior develop a reference threat encompassing all relevant scenarios pertaining to the local authority election process, thereby establishing a foundation for the preparation against these threats.



It is recommended that the Ministry of Interior, in collaboration with the Israel National Cyber Directorate, enhance its detection and monitoring capabilities to identify attacks across all systems employed in local authority elections. This enhancement should include the definition of application and infrastructure monitoring protocols that ensure a comprehensive response to all identified threats, the operation of a central Security Operations Center (SOC) that aggregates monitoring results from all components of the systems supporting election day, and the establishment of preventive measures to be enacted upon event identification.



The Ministry of Interior, the Population and Immigration Authority, and the National Digital Agency ought to collaboratively address the deficiencies that were raised in the context of logical defense.



It is recommended that the Ministry of Interior and the National Digital Agency rectify the deficiencies concerning the interfaces.



Pursuant to the guidelines set forth by the Government Cyber Defense Unit, the Supervisor Unit must ascertain the implementation of access controls designed to safeguard all equipment and information (documents, computers, communications equipment, etc.) from unauthorized physical access. Furthermore, meticulous attention is required to protect sensitive materials. It is suggested that the Supervisor Unit refine the guidelines relating to the transportation, storage, and protection of sensitive election materials in conjunction with relevant stakeholders (e.g., locations for storage, types of structures utilized, and necessary security measures) and oversee their execution. Additionally, it is proposed that the Unit instruct the transportation of sensitive election materials in secured packaging.



It is recommended that the Population and Immigration Authority conduct a situational assessment regarding the deployment of System C on election day and address any identified gaps in System C. Furthermore, it is recommended that the Supervisor Unit



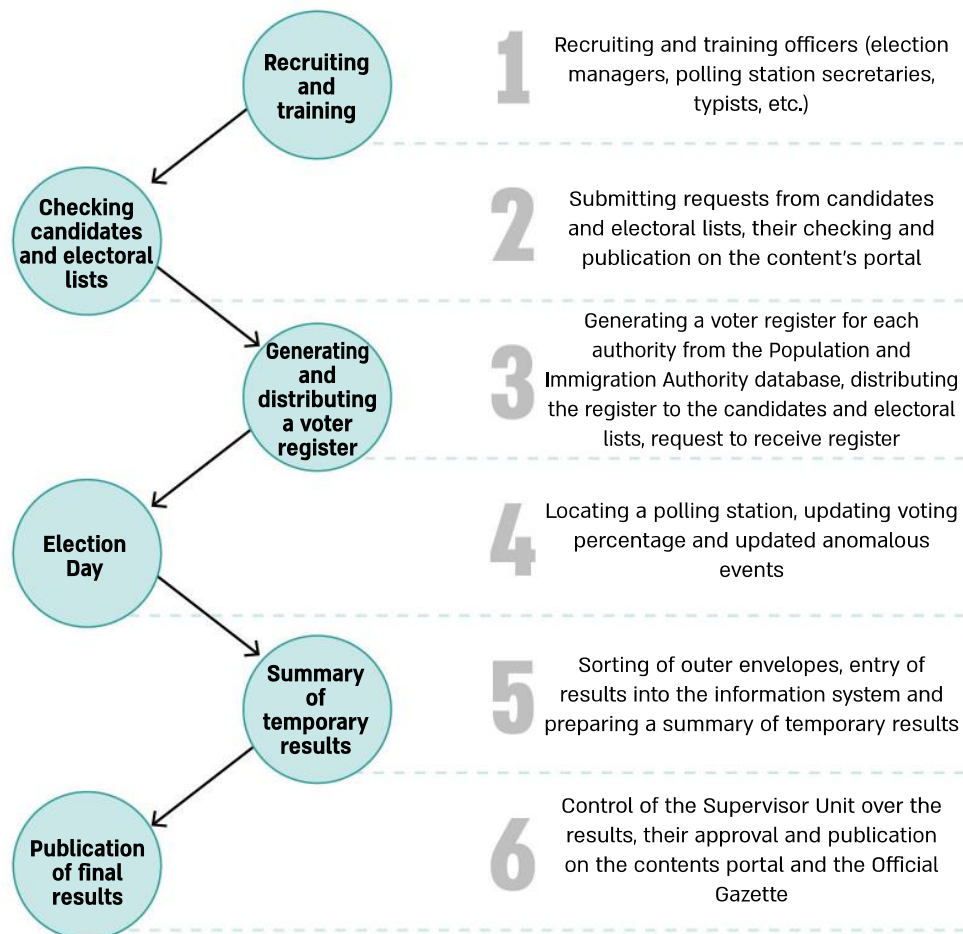
manage potential risks and evaluate the necessity of utilizing temporary remote stations for System C, given the Unit's limited engagement with the system on election night, as the establishment of such temporary stations may pose risks to the sensitive system.



It is recommended that the Ministry of Interior (specifically the Supervisor Unit in collaboration with the Senior Department of Digital Technologies and Information) facilitate the development of an updated election management system intended for forthcoming elections. Accordingly, a work plan should be formulated expeditiously, outlining milestones and timelines to secure all necessary approvals for developing the system in a cloud environment, implement security measures in compliance with the Government Cyber Defense Unit guidelines, and conduct penetration testing at a timing conducive to enabling substantial corrective actions, the integration of requisite compensating controls (including within cloud tools), and the setting of system configurations well in advance of the election dates. Moreover, it is recommended that, in accordance with the system development methodology, interim products be generated (for instance, control findings from elections conducted in one local authority) that may be evaluated and utilized prior to the comprehensive elections (to be held in local authorities throughout the country at the same time), thus ensuring that the system effectively supports all electoral processes and addresses the challenges and errors present in previous electoral systems. Additionally, it is recommended that prior to the election date, the Supervisor Unit, in coordination with election managers, verify, as part of a general rehearsal, the accuracy of all election management systems, including the specification of access permissions for all personnel as well as candidates and candidate lists within the systems, to guarantee system readiness on election day.



Key Processes in Municipal Elections



According to data from the Ministry of Interior, processed by the Office of the State Comptroller.



Summary

Municipal elections serve as a cornerstone for local democracy, and the outcomes of these elections significantly influence various aspects of the daily lives of residents in the State of Israel. The successful management of this national project necessitates the establishment of robust and secure computer systems that thoroughly support each stage of the electoral process.

The Office of the State Comptroller conducted a real-time audit of the information systems and cybersecurity measures during the elections held in February 2024, accompanying the entire process from the preparation phase to election day and the subsequent days. The audit identified deficiencies in both the IT preparations for the elections and the actual conduct during the electoral process, including:

1. A considerable portion of the procedures executed during the electoral process remains manual rather than automated, particularly in relation to voter identification. Technological advancements facilitate a transition to digital identification, anticipated to occur in the coming years. This transition mandates early preparations that establish a foundation for harnessing the benefits of digital identification while also addressing necessary legislative changes and mitigating potential information security risks.
2. The lack of an integrating state regulatory body in the realm of information security and cyber protection that provide guidance and support the election process, ensuring that all systems and infrastructures employed meet the requisite level of protection. This absence is particularly significant given the national scope of the project, which has major implications on the economy that rely on IT infrastructures designated as critical state infrastructures managed by various governmental entities. Compromising those infrastructures could cause the leak of sensitive information pertaining to millions of citizens and disrupt the electoral process.
3. Deficiencies were found in various aspects of information security and privacy protection within the information systems utilized for the electoral process. Some of these deficiencies were presented by the audit team to the Ministry of Interior' in real time and even prior to the elections out of which several deficiencies were rectified during the audit. The Ministry of Interior must continue its efforts to resolve the remaining issues.
4. The development of a new election management system (System A) was not completed by the established deadline. Consequently, the Ministry of Interior opted to cease its development, disbursing NIS 1.8 million for the initial characterization completed thus far (approximately 4.5% of the total projected cost of the project, which was estimated at approximately NIS 40.9 million), and to put into service a previous system (System B). The timing of this decision did not permit adequate testing prior to its implementation, resulting in significant problems identified on election night that ultimately delayed the entry and publication of the election results.



The deficiencies raised in this audit underscore substantial vulnerabilities in the management of the local authority election process that require a response. The findings prompt consideration of the need for ongoing and mandatory guidance and oversight by a governmental entity to provide a comprehensive protective framework for all systems and infrastructures integrated into this significant national project.

The Director General of the Ministry of Interior and the National Supervisor of Local Elections, in collaboration with state regulatory bodies (such as the Israel National Cyber Directorate and the Privacy Protection Authority) and other stakeholders in the electoral process (including the National Digital Agency and the Population and Immigration Authority), must conduct an in-depth analysis of all deficiencies identified in this report and implement rectification measures within a timeframe that guarantees proper and improved ICT management for the subsequent election cycle. To achieve this objective, rectification actions should be incorporated into the annual work plans of the Ministry of Interior and the Supervisor Unit until the next election cycle is conducted.

It is recommended for the Minister of Interior to revive the activities of the Committee for the Computerization of Electoral Systems for the Knesset and the Local Authorities, originally initiated in December 2013 and suspended in 2014. The Minister should advance actions on this matter in agreement and collaboration with the Supervisor Unit and the Central Elections Committee. This initiative will facilitate knowledge-sharing regarding the primary processes and systems employed in various types of elections, as well as those common to all. Given that these two entities are actively seeking to replace the election management systems, the potential for automating certain processes or segments through integrated systems will be evaluated, considering scheduling, cost considerations, the capability to operate multiple election systems concurrently, and cybersecurity and system resilience concerns.

Examples of processes that could be automated, some of which have been implemented at the Central Elections Committee, include, biometric voter identification, automation of nomination forms (legislation is being advanced in this regard), management of minutes of polling station secretaries, establishment of a voter list management system, computerized oversight of polling committee composition, and the application of artificial intelligence technologies. The computerization of the electoral process promises to optimize time and human resource utilization; enable analysis and processing of extensive databases; improve information security, particularly for sensitive data, and reduce the need for its physical transmission; facilitate control procedures; increase transparency and deterrence; and reduce the risks of human error and of compromising the integrity of elections.