State Comptroller's Report – Cyber and Information Systems | May 2023

The Ministry of National Security – The Israel Prison Service

Digital Technologies and Information and Cyber Protection in the Israel Prison Service

Digital Technologies and Information and Cyber Protection in the Israel Prison Service

Background

The Israel Prison Service (IPS) is the national correctional organization, a security body, part of the law enforcement system and subordinate to the Ministry of National Security. The IPS was established in 1949 and, in 2006, was recognized as the State of Israel's national correctional organization. The IPS holds about 14,000 criminal, security, and administrative prisoners and detainees (and another 5,200 prisoners and detainees in incarceration alternatives and under supervision, under IPS responsibility) to protect peace and public security. As of the beginning of 2022, the IPS manages 30 incarceration facilities nationwide (22 prisons and eight detention centers), divided into three command districts – North, Center, and South, and employs 9,200 people. Its annual budget for 2022 was NIS 4.6 billion.

The IPS faces many technological challenges, and to cope with them, it operates through its Technological Division dozens of computerized organizational systems: Operational core systems for prisoner management and intelligence; Medicine and rehabilitation; Personnel, training, and logistics; Diverse security systems installed in incarceration facilities to protect them; Information security and cyber protection systems; And computerized systems in infrastructure, including server farms and a backup site. In 2006−2014, the IPS promoted a project to develop an organizational ICT system (the "Kidma" Project), which failed and was discontinued after an investment of NIS 144 million NIS therein. Beginning in 2021, under the IPS Commissioner's leadership and the Technological Division's Head, the IPS started implementing a strategic move designed to lead to a technological leap in the IPS. This strategic move was expressed in the formulation of the multi-year "Kabarnit" plan (the "Kabarnit" Plan), and its implementation began at the beginning of 2022. This plan, according to the IPS, is intended to shape and lead the IPS' new path as a dominant, innovative, and sophisticated security organization, and among other things, to establish an advanced and innovative work environment for the staff while increasing the use of technology, digitization, and innovation.

Key Figures

13%

the decrease rate in the scope of the IPS technological budget in 2018–2021, while the total IPS budget increased by 12% in those years, and the average technological budgets of government ministries increased by 25%

NIS 0.5 billion

the multi-year budgetary cost to implement the "Kabarnit" plan, of which NIS 400 million is a technological budget

75%

of the technological budget needed to realize the "Kabarnit" plan has not yet been budgeted (NIS 300 out of NIS 400 million)

38%

the actual budget realization rate for the technological projects in the "Kabarnit" plan, planned for 2022 (NIS 39 million out of NIS 104 million). For another 62% of the budget, purchase orders were issued but have not yet been completed

Audit Actions

From March to December 2022, the State Comptroller's Office audited digital technologies and cyber protection in the IPS. The audit includes three tiers as follows:

1. The digital technologies and information systems at the IPS. Including the budget for technology and technological governance at the IPS.
2. Information security, information, and cyber Protection in the IPS.
3. The functional continuity of the IPS technological systems and its effects on the functioning of the prisons in the event of a disaster.

The audit was carried out at the IPS Commission and in various prisons. Completion examinations were carried out at the Ministry of National Security, the National Digital Agency at the Ministry of Economy and Industry, the National Cyber Directorate (NCD) at the Prime Minister's Office, the Budget Division at the Ministry of Finance, and the Israel Security Agency (ISA). The State Comptroller conducted resilience checks on the IPS systems, and the findings were sent to the relevant bodies. The State Comptroller's Office conducted previous audits on various aspects of the IPS activities: "Establishment of an Information System in the Prison Service – the Kidma Project,"; "The Medical System for the Treatment of Prisoners in the Prison Service"; "Criminal Arrests in Israel"; And "Rehabilitation of Prisoners in Israel." Their findings and recommendations were published in the above audit reports.

The Knesset State Audit Committee sub-committee decided not to bring this report in its entirety before the Knesset but to publish only parts thereof to protect the state's security under Section 17 of the State Comptroller's Law, 1958 [Consolidated Version].

Part A – Digital Technologies and Information Systems in the IPS

Key Findings

- **Drawing Lessons from the Kidma Project –** in the eight years since the failure of the Kidma project, an organizational ICT project that failed after the investment of NIS 144 million, the IPS Commission and the Ministry of National Security have not examined the failure reasons nor drawn lessons in management preparations for future computerized projects and the realization of a new organizational ICT project in 2022 – the "Kabarnit" multi-year plan.

- **The Israel Prison Service's ICT Array and Technological Governance –** in 2014–2021, after the failure of the Kidma project, the IPS organization's management was limitedly involved in the ICT array. In 2018–2021, the IPS scope of the technology budget decreased (13%) while the overall budget of the IPS increased by 12%, and the average technological budget of government ministries increased by 25%. Moreover, core positions were partially staffed (the Head of the Technological Division and the Head of the ICT Department in the division). Furthermore, a substantial technological gap was found because of a lack of ICT infrastructures, which did not allow responding to the functional needs and challenges of the organization. As a result, a large part of the management routine of the prisons was done manually. The organization's control systems did not respond to its operational and administrative needs; The means of identifying the prisoners, the array of cameras, and the technological infrastructure on which the organization was based were outdated. This situation adversely affected the functioning of the IPS and its ability to meet its goals.

- **Approval of the "Kabarnit" Multi-Year Plan and its Budget –** the IPS began implementing the "Kabarnit" multi-year plan without the approval of its total budget at half a billion NIS and the approval of the Ministry of National Security and the Minister of National Security for its full implementation. Therefore, the IPS has begun implementing a comprehensive ICT program, with the approval of only about 20% of the total budgetary – NIS 532 million (of which about NIS 400 million is a technological

component), and without the approval of the level in charge of the plan as a whole. This poses a risk to the completion of the plan in the coming years. The IPS decided to implement the multi-year plan despite the lack of a budgetary source and without the Ministry of Finance and the Ministry of National Security committing to allocate the budget to the plan that would ensure its implementation.

Realization of the Technological Division Budgets of the "Kabarnit" Multi-Year Plan and Compliance with the Schedules for 2022 – as of the end of December 2022, the IPS is behind in the realization of the projects in the "Kabarnit" multi-year plan that was planned for 2022. It was found that, out of a budget of NIS 104 million, about NIS 39 million, only 38% of the "Kabarnit" multi-year plan budget was realized. For about NIS 63 million, about 62% of the budget, purchase orders were issued, but the task was not completed. By a breakdown by projects, out of 31 technological projects in the "Kabarnit" plan, 24 projects are executed as planned, and 7 projects are behind schedule, among other things, as the budget from the Ministry of Finance was not received on time. The main projects whose implementation is delayed are the salary and personnel project, the server farm, the computerized prisoner file, visual conferencing with the courts, and the C&C system.

ICT Risk Survey – despite the technological complexity of the IPS ICT array, the scope of the information systems, and their interfaces with government bodies, the IPS did not map the information assets, databases, infrastructures, and projects, nor did it conduct ongoing and comprehensive risk surveys. It was also found that the IPS did not perform comprehensive risk management of the "Kabarnit" plan for dealing with systemic risks in the budget, schedules, interfaces, infrastructure, technology, personnel, information security, assimilation, and the interdependence between the plan's components. A dedicated ICT risk manager was recruited only at the beginning of 2023.

Investing in Technological Advancement – after a long period of technological stagnation, starting in 2021, the IPS, and in particular its Technological Division, is investing considerable effort to catch up on the technology gaps by initiating and implementing projects to promote digitization at the operational and administrative core of the organization.

Restructuring and Addition of Technological Personnel – as part of the "Kabarnit" multi-year plan, a restructuring was carried out in the Technological Division. Furthermore, in 2022, personnel recruitment began and was largely completed, leading to a doubling of the personnel in the Division from 100 to 199 contractor employees.

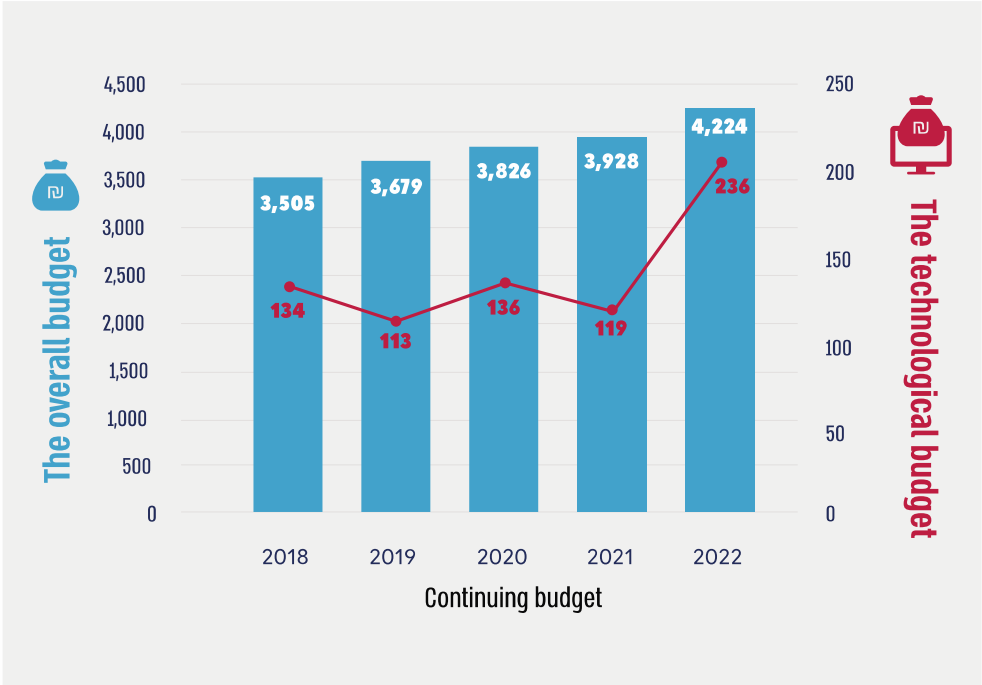
Implementation and Integration of Technologies in the Operational Core Systems – in 2022, the Technological Division, as part of the "Kabarnit" multi-year plan,

implemented new technological systems such as digital diaries, a digital prisoner file, and multidimensional monitoring systems as part of the transition to a "smart prison".

Key Recommendations

- It is appropriate that the Israel Prison Service implement an organizational methodology of investigation and drawing lessons for future computerized projects. It is recommended that this process also apply to the "Kabarnit" plan as a whole, considering its cost and complexity. The Ministry of National Security, in charge of the IPS and guiding it, should be involved in these processes.
- It is recommended that the minister and the Ministry of National Security examine the "Kabarnit" plan for its approval, including the multi-year budget for its implementation. It is also recommended that the Ministry establish a regular and ongoing arrangement for monitoring the implementation of the program's core projects, including their goals, contents, timetables, and budgetary implementation. The performance of the "Kabarnit" plan, which is a multi-year and resource-intensive plan, requires the IPS to realize the plan after receiving approval from the Minister and the Ministry of National Security for the plan as a whole.
- The IPS should implement the National Digital Agency guidance and conduct a comprehensive and ongoing risk survey of all its activities, including the "Kabarnit" plan that was carried out at the audit time, and complete the project management staffing of the positions.
- It is recommended that the Ministry of Finance transfer development budgets ahead of time and not at the end of the budget year so that government bodies, including the IPS, can use these development budgets and issue orders in respect thereof at the same year, without being subject to budget cuts due to them being "committed surpluses." It is also appropriate that the Ministry of Finance, the Ministry of National Security, and the IPS examine the full range of implications of the "Kabarnit" plan's budget and the IPS technology budget, considering, among other things, the budget challenges at the audit time. All this is to ensure the implementation of the "Kabarnit" plan, given the importance of its completion.

The IPS' Technological Budget Compared to the IPS' Overall Budget and its Changes, 2018–2022 (in NIS millions)



According to the IPS and Ministry of Finance data processed by the State Comptroller's Office.

Part B – Information Security, Information, and Cyber Protection in the IPS

The findings in this audit chapter are not made public to protect state security

The IPS, the national correctional organization that oversees 30 incarceration facilities, is a security body that holds thousands of criminal and security prisoners in custody. The information about these prisoners, including classified security information and sensitive personal information in the medical, biometric, and intelligence fields, is managed in the organization's information systems. Furthermore, the IPS computers store much information on modus operandi, operations, investigations, and information on the IPS defense and security systems. In addition to the information originating from the organization, the IPS receives classified, operational, and intelligence information from the Police and other agencies. The disclosure of this information to an unauthorized party may result, among other things, in harm to the state, risk human life, the disclosure of information, methods of operation, and covert investigations, and in the foiling of operations.

In recent years, a significant increase in cyber incidents has disrupted the everyday activities of organizations in Israel and worldwide. There is also a marked increase in the severity of these incidents.

Key Findings

The Regulation of Professional Guidance in Information and Cyber Protection

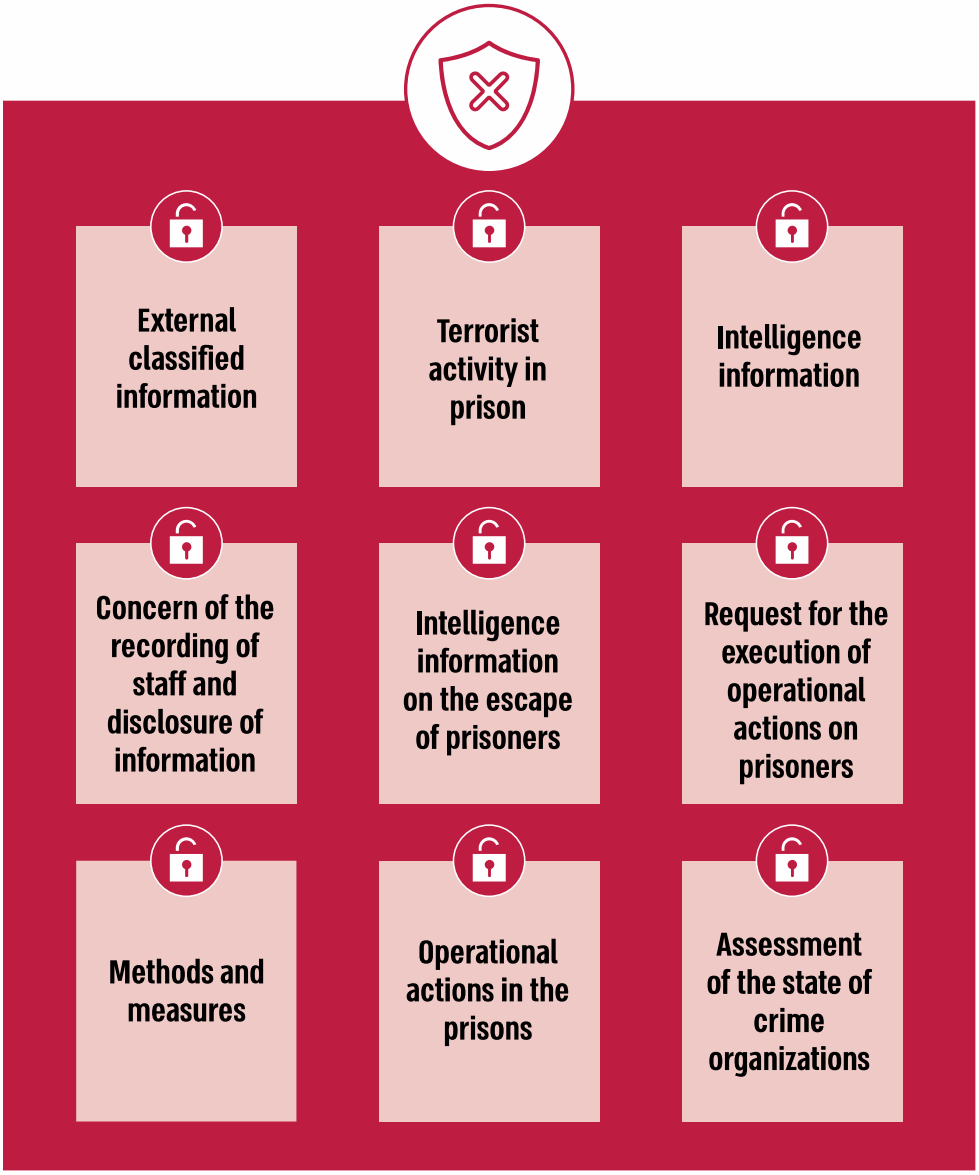
- **The Body Guiding the IPS in Information and Cyber Protection –** The IPS is a security body whose systems contain classified information at different levels. It was found that over the years, the IPS, the Ministry of National Security, and the National Cyber Directorate were not aware of the rules established in 2004 by the Prime Minister, which assigned the IPS with the responsibility of determining for itself the methods of securing classified information under the principles defined. Therefore, regarding the classified data, which embodies the highest risk, the IPS did not act under the binding rules or lay the necessary foundation for handling this sensitive field. In addition, the IPS did not receive support and guidance on classified data, even though regarding its

unclassified data, which embodies a lower risk, it received support and guidance from the sectoral unit in the Ministry of National Security. Moreover, despite the Israel Prison Service being a security body and the sensitive information in its possession, the Top Steering Committee for the Protection of Critical Computerized Systems (Committee B/84) did not discuss the IPS. It did not examine whether it should be defined as a "critical" body needing cyber Protection.

- **The Cyber Protection Policy –** the IPS was obliged to publish an organizational cyber security policy under the government's resolution in 2015. It was raised that at the audit completion in December 2022, the policy was approved for publication by the Deputy Commissioner as an organizational thematic doctrine but has not yet been approved by the sectoral unit in the Ministry of National Security. Furthermore, the approved sectoral policy document, which was published by the Ministry of National Security and which is intended, among other things, to direct and guide the bodies under its responsibility in cyber protection, is partial and does not include detailed instructions, adapted to accepted norms in the cyber Protection, for the bodies under its responsibility. The lack of these instructions affects the ability to ensure adequate preparedness of the IPS to cope with cyber-attacks.

- **The Management and Security of Classified Security Information –** one of the guiding principles for the security of classified information and documents is that there is a real need for compartmentalization and security measures to prevent the disclosure of security-sensitive information to an unauthorized party. The document's security sensitivity degree is determined by its classification level. Top Secret, Secret, Restricted, and Unclassified are the four classification levels.

Examples of Information on the IPS Networks



The State Comptroller's Office examined a series of management and security aspects of classified security information. This examination raised significant gaps contrary to the binding practice in equivalent bodies. These gaps were found in each of the following areas:

1. Processing classified digital information and classified documents.
2. Regulating the handling of classified security information through security procedures, keeping and classifying documents.
3. Processing of classified information received from external sources.
4. Regulating the security clearance of employees in the IPS.
5. Use of means of communication.

Protection of ICT Systems and Infrastructures

The State Comptroller's Office examined a series of protection of ICT systems and infrastructure aspects at the IPS. Penetration tests were also carried out with a vulnerability assessment survey of the IPS networks. Significant gaps were raised in this examination, contrary to the binding practice in equivalent bodies. These gaps were found in each of the following areas:

1. The cyber security of some systems.
2. Conducting risk surveys in information and cyber protection and conducting penetration tests.
3. Preparation for managing cyber incidents.
4. User management and permissions management.
5. The development processes of a classified computer network.

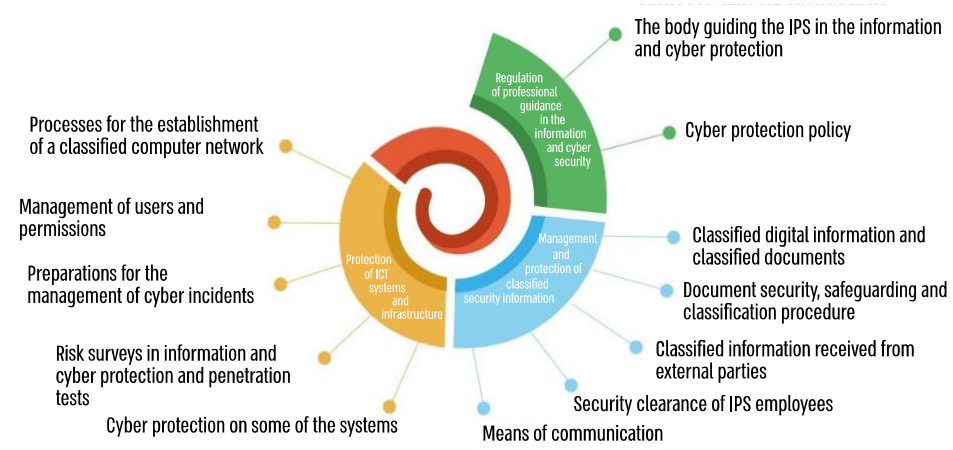
The extensive activity in the IPS Cyber Protection Department in recent years for implementing secure architecture and protection solutions is commended. This is despite the limited resources available to the IPS. This activity considerably improved information protection.

Furthermore, in 2021 and 2022, the IPS allocated over 8% of the organization's total annual information technology budget to the cyber security, meeting the minimum rate set by the government resolution.

Key Recommendations

This chapter raised significant gaps in managing classified security information and its protection in the IPS computer systems. Moreover, the report raised a long-standing reality whereby the areas of responsibility and authority of the IPS and the regulators of classified information and cyber security, and in digital technologies and information systems, are not implemented, properly as required. It is recommended that the Prime Minister, in consultation with the Minister of National Security, examine the IPS information and cyber security as a whole, particularly the classified information security. Until the Prime Minister's decision, the IPS should comply with ISA rules.

The key Gaps in the Information Security, Information and Cyber Protection



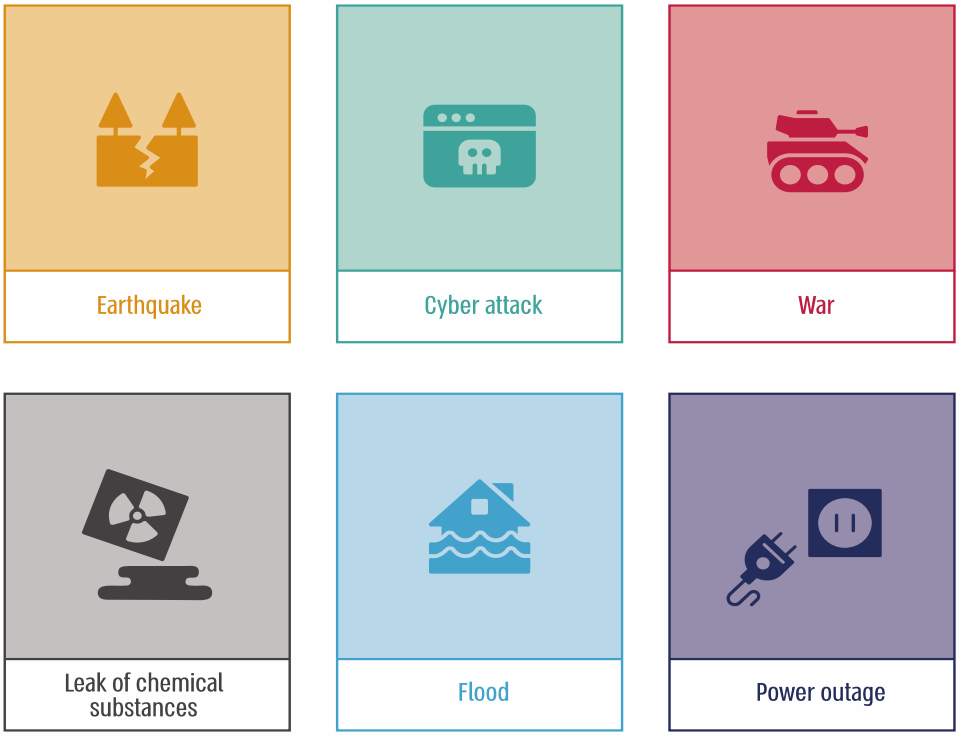
According to the audit findings, processed by the State Comptroller's Office.

Part C – The Functional Continuity of the IPS Technological Systems and its Effects on the Prisons Functioning in the Event of a Disaster

The findings in this audit chapter are not made public to protect state security

The functional continuity of the IPS in a variety of critical administrative and operational processes, including the security of the prisons at all levels, including the management of the intelligence system, the management of the day-to-day routine in the prison, including the counting of prisoners, distribution of medication to prisoners, personnel management, all depends on the technological systems. This continuity may be affected by a disaster or a severe crisis, whether it is a crisis that can sometimes be expected (such as a severe storm or extreme weather) or whether it is an unexpected crisis (such as a power outage, earthquake, terrorist event, war or accident) that disrupts the organization's routine. These events may also cause severe damage to the organization's technological system and create failures therein. Severe damage to the technological system can also result from physical damage (in good faith or with malice) or cyber-attacks on the organization's technological infrastructures and systems. Since the IPS is required to keep prisoners in safe custody even during an emergency or disaster, it should be prepared and ready for various emergencies and provide a response of functional continuity in any situation.

The Main Disasters at the Basis of the IPS' Threat Reference



Key Findings

The State Comptroller's Office examined a long series of the functional continuity of the technological systems aspects in the IPS and their effects on the functioning of the prisons in the event of a disaster. The examination raised significant gaps contrary to the binding practice in equivalent bodies. These gaps were found in each of the following areas:

1. The technological response to the threat reference.
2. The Business Continuity and Functional Continuity Plan at IPS.
3. The Disaster Recovery Plan at IPS.
4. Protection of a sensitive IPS site and its operation.

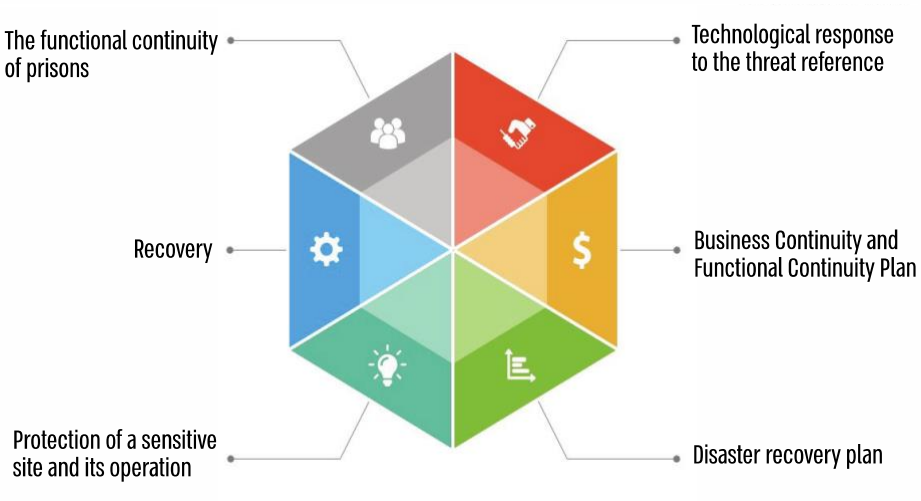
5. Data recovery and information systems recovery from backup.
6. The functional continuity of the prisons.

The IPS effort to promote and prioritize the establishment of the new server farm is commended.

Key Recommendations

The functional continuity of the IPS is of strategic importance in terms of the lives of the prisoners in its custody and the guards entrusted with their custody and in the security and social aspects. The IPS and the Ministry of National Security should rectify the gaps raised in this chapter and implement detailed recommendations, all to ensure that this continuity is not affected by the occurrence of catastrophic events that may endanger the stability and functioning of the national correctional organization.

The Key Gaps in the Functional Continuity of the IPS Technological Systems and its Effects on the Functioning of the Prisons in the Event of a Disaster



According to the audit findings, processed by the State Comptroller's Office.

Summary

The Israel Prison Service provides safe custody of prisoners and criminal and security detainees under adequate conditions while maintaining their dignity and rehabilitation toward integration into society following their release. Advanced technological systems support prison systems operating worldwide in realizing these organizations' mission. The role of the IPS, realizing its mission and security nature, requires it, similar to prisons around the world, to use advanced technological systems.

The IPS organization's management was limitedly involved in information technologies; moreover, a low technology budget, partial staffing of core positions, and a substantial technological gap affected the IPS's functioning and ability to meet its goals. At the end of 2021, the IPS was in a significant technological lag, in contrast to the benefits inherent in technological means as a tool to improve its ongoing administrative and operational functioning. In 2022, changes were executed to minimize the organization gaps to achieve a technological leap. The IPS, led by the Commissioner, adopted a comprehensive multi-year plan to improve the technological array. It even began its implementation in 2022 while receiving partial budgets from the Ministry of National Security and Finance. However, the plan, which was defined as a multi-year plan, did not receive the approval of the Minister of National Security on time and was only budgeted for its first year without a commitment being made by the Ministry of Finance and the Ministry of National Security to continue its budgeting in the coming years and to ensure its full realization.

The Minister and the Ministry of National Security are responsible for the functioning of the incarceration array in Israel, and they should ensure that the IPS fulfills its role through appropriate technological infrastructure and that the building up of that force is managed with a long-term vision and a budget outline that guarantees its implementation. In cooperation with the Ministry of National Security and the Ministry of Finance, the IPS should continue to reduce the existing technological gaps and place the IPS at an advanced technological level that matches its responsibility and mission as a security organization. The IPS should execute an orderly process of drawing lessons from previous failures in this area, manage ICT risks in general and the "Kabarnit" multi-year plan in particular, and provide a supportive professional management environment for its implementation.

This report also highlights significant gaps in managing classified security information and its security in the IPS computer systems. Despite the IPS being a security body, the computing infrastructure does not comply with the standards required of security bodies. The report raises a long-standing reality whereby the responsibility and authority of the IPS and the regulators in the classified information and cyber security, and the digital technologies and information systems, are not implemented properly and as required. This report is a warning sign for all bodies involved in securing state secrets, information, and cyber security and requires quickly rectification of the gaps raised therein. It is recommended that the Prime Minister, in consultation with the Minister of National Security, examine the information and

cyber protection in the IPS as a whole, particularly the classified information security. Until the Prime Minister's decision, the IPS should comply with ISA rules.

The functional continuity of the IPS is of strategic importance in terms of the lives of the prisoners in its custody and the guards entrusted with their custody and from the security and social aspects. The IPS and the Ministry of National Security should ensure that this continuity is not affected by catastrophic events that may endanger the stability and functioning of the national correctional organization.

It is recommended that this report be studied and that lessons be drawn from it for other government bodies of a similar nature in information security, information, and cyber security, as well as functional continuity of the technological systems and disaster preparedness.