Report of the State Comptroller of Israel | May 2024

Israel Land Authority

Information Security and Cyber Protection at the Israel Land Authority

Information Security and Cyber Protection at the Israel Land Authority

Background

The Israel Land Authority (ILA) manages Israel's land as a resource, under the Israel Land Authority Law, 1960, for the development of the State of Israel and the benefit of the public, the environment, and future generations.

Most of the information ILA collects, stores, and manages is sensitive information about real estate assets, including personal and business data. Furthermore, ILA operates a website that provides service to the public. ILA has the duty to protect the information in its possession and ensure that it is used only for the purposes for which it was provided or to fulfill its obligations according to the law. Concerning the real estate assets, ILA is required to protect the confidentiality of the information, its trustworthiness, availability, and reliability, and ensure that the data is not altered or deleted and that it is disclosed only to those authorized to access them according to their position or because the information concerns them.

Regarding the protection of privacy and the security of the significant amount of information in its possession, ILA must comply with the law's provisions, including the Protection of Privacy Law, 1981 (Protection of Privacy Law), and the regulations promulgated thereunder. According to ILA's mapping, its threats include internal threats, for example, from its providers, and external threats, such as hackers and customers.

Key Figures

dozens

of information systems, ILA uses to manage its activities

millions

of scanned files are stored on ILA's servers. These include tens of millions of documents, mainly of rights to Israeli lands, including lease contracts, payment confirmations, and inspection reports

2019

the last year in which the Cyber Steering Committee at ILA discussed and approved the information security policy, despite significant changes since the policy was approved

12%

of the budget for ILA's computing expenses in 2022 was earmarked for information and cyber security

hundreds of thousands

of entries to the ILA website are made every month

only 5

the Cyber Steering Committee discussed and examined the compliance of only 5 cyber protection master indices, out of ten (50%) in 2022

5

ILA databases that are supposed to be registered in the Databases Register to ensure the privacy protection of their information were not registered

Audit Actions

From February to October 2023, the State Comptroller's Office examined aspects of information security and privacy protection in ILA's information systems, including governance and management of information and cyber security, database registration, and business continuity plan and disaster recovery plan. The examination was carried out at ILA.

The Knesset State Audit Committee sub-committee decided not to submit parts of this audit to the Knesset and publish only parts thereof to safeguard the state's security under Section 17 of the State Comptroller’s Law, 1958 [Consolidated Version].

Key Findings

- **Steering Committee for Cyber Protection –** since the ILA Cyber Steering Committee first convened in 2017, it has not approved, mapped, and classified ILA's information assets. Moreover, although many risk surveys were carried out, the Cyber Steering Committee did not discuss plans to address or mitigate them, including contents, execution schedules, responsibilities, and required resources. Furthermore, the Steering Committee did not initiate or compile management surveys as needed. It did not convene as often as required under the government's resolution, impairing the ability of ILA's management to optimally control the efficient and effective implementation of cyber protection at ILA and the extent to which the work plan for the management of ILA's cyber protection is suited to the risk level of each system.

- **Information Security Policy and Annual Cyber Protection Work Plan –** ILA's cyber protection policy was approved by the Cyber Steering Committee in 2019, and since then, it has not reviewed, updated, or discussed them, despite significant changes that have taken place since 2019 in ILA's computer system, and despite technological developments in the world. Moreover, the work plan presented to the Cyber Steering Committee only included the details of the topics planned for implementation. It did not include schedules, parties responsible for implementation, budget, and priorities. Furthermore, there are no documents attesting to the Committee's monitoring of the implementation of the plan, including rectifying the deficiencies raised in the risk surveys and the penetration tests carried out.

- **Determining Indices on Cyber Protection and Meeting Them –** in its meeting in May 2019, ILA's Cyber Steering Committee approved ten master indices on cyber protection. For example, an index for information security awareness is that 80% of employees must participate in information security training. The audit raised that from 2019 until the audit end date (October 2023) – over four years – the Committee examined the degree of implementation of the indices only twice (in December 2019 and December 2022) and not every six months as required. As a result, its ability to examine the effectiveness of the cyber protection infrastructure was impaired, and accordingly, its ability to make relevant changes more frequently as required. Moreover, only a part of the master indices approved in May 2019 were presented in the Cyber Steering Committee discussions in December 2019 and December 2022. In December 2019, six of the ten approved master indices were presented to the Committee (about 60%), and in December 2022 – only five (about 50%).

- **Registering the Databases –** in 2019, the Cyber Steering Committee approved the appointment of five managers for current databases, and database definition and structure documents were prepared for these databases. However, ILA did not register these databases, as required by law, even though about five years have passed since it recognized the need to do so, and as of the audit end date, the five databases had not yet been registered. Moreover, the Steering Committee did not discuss the reasons for failing to register the databases.

👎 **Management of Access Privileges to the Databases and Access Control –** the Privileges Committee established pursuant to the Cyber Steering Committee's decision did not convene, and the access privileges matrix was determined by ILA's Information Systems Division, without the approval of the Privileges Committee and without the involvement of the database managers who are tasked with determining the privileges. The audit raised that there is a certain control mechanism in ILA, but it does not provide alerts in respect of certain actions. As a result, the control mechanism is not optimal and does not comply with the requirements.

👎 **Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) –** since the Cyber Steering Committee first convened in 2017, preparing for a disaster recovery plan has been on the agenda in all its meetings. However, it neither discussed nor adopted operative decisions about the above plan. Moreover, the progress in preparing the plan was not presented to the Committee in the annual activity summaries.

👎 **Alternative Site in the Event of a Disaster (DR) –** ILA's information systems are located on several sites. In the summary of the information systems infrastructure risk survey carried out by ILA in March 2019, various risks were noted regarding a particular site.

👍

Conducting Penetration Tests – in 2017–2022, ILA carried out dozens of risk surveys and penetration tests for its information systems. However, the risks raised in the penetration tests were not brought before the Steering Committee.

Protection Level According to the Government Cyber Protection Unit (YAHAV) Test – according to the YAHAV index test report[1] from 2022, ILA is in the top quintile regarding the level of cyber protection. However, gaps were found in five controls, all from the "management responsibility and compliance" tier.

[1] A uniform test index for government organizations in the field of information security and cyber protection formulated by the Government Cyber Protection Unit.

Key Recommendations

- ILA should bring the mapping and classification of its information assets and cyber protection policy to the Cyber Steering Committee for approval and complete the risk surveys for its systems. The Cyber Steering Committee, led by the chairman (ILA's Director), should formulate management surveys, monitor the execution of work plans in cyber protection, examine its degree of effectiveness at ILA according to the established indices, and ensure it convenes as required under the government resolution.

- ILA should register the current databases as the law requires, and the Cyber Steering Committee should monitor such registration.

- It is recommended that ILA convene the Privileges Committee to regulate the access privileges, including examining whether the privileges for each office holder are according to the position's needs. It is further recommended that ILA involve the database managers appointed by the Cyber Steering Committee in determining the privileges.

- ILA should prepare a business continuity plan, including a disaster recovery plan, based on the principles approved by the Cyber Steering Committee.

- To fully respond to emergency incidents, including ensuring the ability to return to normal and reasonable activity as soon as possible, ILA should rectify the deficiencies raised in this regard.

Summary

ILA manages one of the most essential resources of the state – Israel's land. Most of the information ILA collects, stores, and manages is sensitive information about real estate assets, which includes millions of records, and is therefore required to be secured at the highest level of security. To this end, ILA operates systems and mechanisms to protect its databases and systems, and identify and mitigate risks.

This audit examined the information security and privacy protection in ILA's information systems, including the extent of ILA's compliance with the key rules outlined in the law, the privacy protection regulations, and the Government Cyber Protection Unit (YAHAV) guidelines. It was found that ILA carried out various risk surveys and penetration tests of its systems, and it is rectifying the deficiencies therein. However, the supervision and control of the management of the cyber sector are lacking: among other things, ILA's Cyber Steering Committee, which is supposed to outline a policy in information security and supervise its implementation, keep up to date with risks and threats to ILA and supervise cyber risk management at ILA, did not examine or approve the mapping and classification of ILA's information assets, to maintain optimal control; It did not compile management surveys, to check the quality of information and cyber protection management at ILA; And did not monitor the degree of execution of the work plans as required. Furthermore, it was not presented with the risks found in the penetration tests and the implementation of the mitigation plans.

The audit also raised gaps regarding a specific control mechanism, functional continuity, and disaster recovery.

ILA should rectify the deficiencies noted in this report to strengthen the protection of the information in its possession and increase the effectiveness of its actions.