State Comptroller of Israel | Local Government Audit | 2022

Information systems audit

Management of Information Systems in Local Authorities

Management of Information Systems in Local Authorities

Background

Using IT systems to manage the local authorities' affairs has become a fundamental and essential need. Among other things, the local authorities also use databases that contain residents' personal information and of different entities engaged with the local authorities. The local authorities accumulate residents' personal information, such as names, addresses, ID numbers, phone numbers, medical information, welfare-related information, details about their chosen methods of payment, and unfiltered information, such as license plates, facial features, location data, and movement habits. Local authorities face different risks, including loopholes in their information security systems and cyber threats. Their information systems have become an attraction for hackers and cyber offenders. Thus, it is essential to safeguard their information systems to ensure operational resilience, which is focused on the continuity and recovery of critical business processes of the local authorities, data and information leakage from their databases, and their exposure to unauthorized entities.

Key figures

67%

rate of local authorities (87 out of 130) whose achievement in the cyber resilience test conducted by the Cyber Department in the Ministry of Interior was below 60

61%

rate of local authorities with no cyber-event recovery plan upon DRP/BCP (36 out of 59 that answered this question in the questionnaire)

108

the accumulated number of queries submitted by 32 local authorities to the Cyber Emergency Response Team (CERT) (at the National Cyber Directorate) in 2019–2021

41%

rate of local authorities that experienced cyber events (successful or failed ones) in 2019–2021 (24 out of 59 that answered this question in the questionnaire)

34%

rate of local authorities that did not appoint a Chief Information Security Officer (CISO) (21 out of the 61 that answered this question)

64%

rate of local authorities with no information security procedure (37 out of the 58 that answered this question)

18%

rate of local authorities that did not appoint a CISO (11 out of the 61 that filled in the questionnaire)

49%

rate of local authorities that did not conduct Penetration Tests (PT) in 2019–2021 (30 of the 61 that filled in the questionnaire)

Audit actions

From July to November 2021, the State Comptroller's Office examined information system management in local authorities. The audit was conducted at eight local authorities, considering their administrative districts; their municipal status; their socio-economic status; their peripherally status; the sector most of their residents belong to, and the number of residents in their jurisdictions. In five municipalities – Haifa, Yokneam, Netivot, Rosh Ha'ayin, and Shfaram, in two local councils – Gedera and Ein Mahil and in the regional council of Mateh Binyamin (the audited local authorities). Supplementary audits were conducted in the Ministry of Interior – at the Emergency Services Administration and Mifam Emek Yizrael, the Center for Local Government, and the National Cyber Directorate under the Prime Minister's Office (the Cyber Directorate). Moreover, questionnaires were sent to 63 local authorities, and 61 (97%) of them filled in the questionnaire.

Key findings

- **Tests conducted by the Ministry of Interior Cyber Department** – it was found that by August 2021, the Ministry of Interior Cyber Department had completed basic tests in 130 out of 257 local authorities. It was further raised that 87 (approx. 67%) out of the 130 achieved a grade lower than 60, only 11 (8%) achieved a grade higher than 80, and the average grade was 48. Therefore, the level of information security and cyber threat preparedness of most local authorities (67%) is low, and the local authorities examined by the Ministry of Interior significantly differ in their preparedness for cyber-attacks.

- **Reports to the CERT (at the Cyber Directorate)** – the Cyber Directorate data regarding local authorities' queries indicate that in 2019 there were 32 queries by 14 local authorities. In 2020, there were 40 queries made by 25 local authorities, and in 2021, there were 36 queries made by 19 local authorities. Overall, in 2019–2021, there were 108 queries made by 32 local authorities (out of 257).

- **Responsibilities division between the Ministry of Interior and the Cyber Directorate** – the Ministry of Interior and the Cyber Directorate have not completed to define the roles and responsibility regarding regulation and professional guidance for local authorities on information security and privacy protection. In addition, the Ministry of Interior has not prepared a policy to guide local authorities in this area. As a result, as of the audit completion date, the local authorities had not appointed an official in charge of information security and protection against cyber threats. For years, the local authorities have been operating without concrete professional guidelines in this area, and each local authority has made its own decisions.

- **Information Systems work plans** – **Gedera**, **Yokneam**, **Mateh Binyamin**, **Netivot**, **Ein Mahil and Shfaram** have not prepared multi-annual, strategic work plans related to information systems or annual budget-dependent work plans according to their long-term objectives. It was further found that **Haifa and Rosh Ha'ayin,** that determined strategic plans information systems, did not allocate budgets for that purpose, thus, the plans were not carried out.

- **Appointing a Chief Information Security Officer (CISO)** – 21 (approx. 34%) out of the 61 local authorities that answered the relevant question in the questionnaire do not employ a CISO as required, and amongst the audited local authorities, **Gedera** and **Ein Mahil** do not employ a CISO.

👎 **Information security policy** – amongst the audited local authorities, **Yokneam**, **Gedera**, and **Mateh Binyamin** did not formulate an information security procedure as specified in the information security regulations. **Netivot**, **Shfaram**, and **Ein Mahil** had only prepared a procedure drafts that had not been approved by the audit completion date.

👎 **Backup procedure formation and implementation** – it was found that amongst the audited local authorities, **Yokneam** and **Rosh Ha'ayin**, **Gedera**, **Ein Mahil**, and **Mateh Binyamin** do not have a backup policy as required. **Netivot and Shfaram** have backup procedure drafts, which have not been approved yet. No records of proper backup history were found in **Yokneam, Shfaram**, and **Ein Mahil**. **Authorization Management** – **Yokneam**, **Ein Mahil,** and **Mateh Binyamin** do not have written rules about granting or denying authorization permissions. **Gedera** has a policy that came into effect in June 2021. **Netivot and Shfaram** have procedure drafts (from July 2020 and July 2021, respectively) that had not been approved by the audit completion date.

👎 **Cyber Event Recovery Plan** – 36 (approx. 61%) of local authorities that answered the question on recovery plans stated they have no regulated mechanism that allows continuous computer function in a cyber-event. The audited local authorities - **Gedera**, **Haifa**, **Yokneam**, **Mateh Binyamin**, **Ein Mahil**, **Rosh Ha'ayin**, and **Shfaram** – have not formed any recovery plans. **Netivot** had developed a draft plan, which, as mentioned, had not been approved by the date of audit completion.

👎 **Security Risk Assessments and Penetration Tests or Periodic Audits** – **Mateh Binyamin** has conducted a Security Risk Assessment to identify information security risks in 2020 but did not conduct database Penetration Tests (PTs). **Netivot** conducted a Security Risk Assessment in 2019 but did not conduct Penetration Tests (PTs). **Yokneam**, **Shfaram**, and **Ein Mahil**, which are not required to conduct Penetration Tests (PTs), did not conduct Security Risk Assessments or periodic audits. It was further found that **Gedera** did not conduct Penetration Tests (PTs) or Security Risk Assessments but instead relied on a private company that provides them IT services.

👍

The State Comptroller Office commends **Haifa**, **Netivot, and Rosh Ha'ayin** for conducting Penetration Tests (PTs) or Security Risk Assessments in 2019–2021.

Key recommendations

- It is recommended that the Ministry of Interior and the Cyber Directorate work together and consider the local government's uniqueness and divide the powers between them to carry out Government Resolution no. 2443. Thus, a leading regulator will be appointed to regulate local authorities' preparedness for cyber threats and set relevant procedure to regulate their function. It is further recommended that the Cyber Directorate of the Ministry of Interior Cyber Department increase awareness of the importance of reporting the CERT cyber events the local authorities are exposed to and the possibility to consult with the Cyber Directorate.

- The Local Authorities of **Gedera**, **Yokneam**, **Mateh Binyamin**, **Netivot**, **Ein Mahil**, and **Shfaram** should form a strategic work plan as a basis of annual work plans, submit it to the authority's management for discussion, ensure it corresponds with its budget, and implement it.

- Given the local authorities are obliged to appoint a CISO, all local authorities who have not appointed one, including **Gedera** and **Ein Mahil**, should do so. It is recommended that the Ministry of Interior guide the local authorities, which did not appoint a CISO to do so, and complete defining a CISO's job description and terms of employment, together with the Center for Local Government.

- **Yokneam**, **Gedera**, and **Mateh Binyamin** should prepare an information security policy as required. Moreover, **Gedera** should ensure that its company's information security policy is approved and, if needed, adapted to the authority's needs. **Netivot**, **Shfaram**, and **Ein Mahil** should approve the procedure and indicate the date on which it comes into effect.

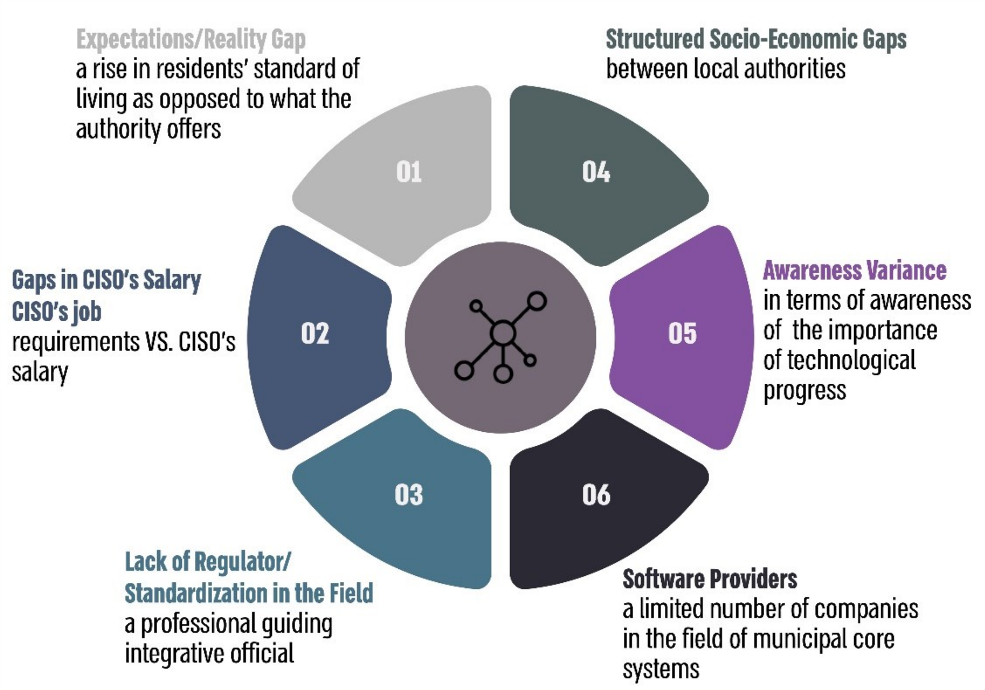
- **Gedera**, **Yokneam**, **Mateh Binyamin**, **Netivot**, **Ein Mahil**, **Rosh Ha'ayin**, and **Shfaram** should set a valid backup procedure and perform the backup as specified in the policy.

- **Yokneam**, **Ein Mahil**, and **Mateh Binyamin** should establish the rules for granting authorization to new employees and employees who leave the authority. **Netivot** and **Shfaram** should approve the draft procedure and act upon them.

- Given the importance of preparing a Disaster Recovery Plan (DRP), the State Comptroller Office recommends all local authorities, including the audited local authorities (**Haifa**, **Yokneam**, **Rosh Ha'ayin**, and **Shfaram**, **Gedera** and **Ein Mahil** and **Mateh Binyamin**), to prepare a Disaster Recovery Plan (DRP) adjusted to the authority's needs, according to the Cyber Directorate guidelines. It is recommended that **Netivot** complete the preparation of the Disaster Recovery Plan (DRP).

Yokneam, **Ein Mahil** and **Shfaram** should conduct periodic audits, preferably as part of Security Risk Assessments, to map and identify information security risks and mitigate them. It is further recommended that the **Yokneam**, **Netivot**, **Ein Mahil** and **Shfaram** conduct Penetration Tests (PTs) even if their databases require a medium level of security.

Main Challenges in the Information System Management in Local Authorities



Expectations/Reality Gap
a rise in residents' standard of living as opposed to what the authority offers

Gaps in CISO's Salary
CISO's job
requirements VS. CISO's salary

Lack of Regulator/ Standardization in the Field
a professional guiding integrative official

Structured Socio-Economic Gaps
between local authorities

Awareness Variance
in terms of awareness of the importance of technological progress

Software Providers
a limited number of companies in the field of municipal core systems

Summary

The local authorities use of IT systems to manage their affairs has become fundamental and essential, but it also involves cyber threats. In addition, the local authorities' databases contain, among other things, the personal information of residents and of different entities engaged with the local authorities, which requires ensuring database security for privacy protection.

In the audited local authorities, various cyber protection and information security deficiencies were found, which derive, among other things, from a lack of strategy and guidance from the entities in charge. Due to the importance of this subject, it is recommended that the Cyber Department in the Ministry of Interior, together with the Cyber Directorate, guide the local authorities to clarify their duties and the recommended modus operandi needed to improve information security. It is further recommended that the local authorities use their available tools to set a general strategy for managing IT systems and improving information security. All local authorities should use all tools available to optimize their IT system management and to enhance their ability to protect sensitive information to ensure operational resilience, focused on the continuity and recovery of their function.