State Comptroller | Annual Report 72A - Part One | 2021

Systemic Issues

Government Ministries use of the Public Cloud and Preparations for the Establishment of a Central Cloud

Government Ministries' use of the Public Cloud and Preparations for Establishment of a Central Cloud

Background

The development of cloud computing technology enables the government sector to better address the many challenges it faces, such as improving service to the citizen, reducing inter-office variability and enhancing operational efficiency. But along with the benefits, the use of this technology also entails real risks in the areas of information security and cyber protection, privacy protection and more.

In recent years, the Government of Israel has recognized the need for forward-looking planning and outlining a vision, goals and objectives that will enable the realization of the potential inherent in cloud technology, and make it easier to deal with the challenges involved in using this technology.

Key figures

2%

Average annual utilization rate of existing local computing infrastructure resources in government in 2018

1%

In 2019, the government invested less than one percent of its total investment in ICT in cloud computing, compared to 8% worldwide[1]

102

Number of systems that have been moved to a cloud environment[2] out of thousands of information systems and computer infrastructures in the government sector

773%

Increase in the number of threats to cloud services of the government sector worldwide in March and April 2020 compared to January and February of that year

60%

Proportion of offices that responded to the State Comptroller's Office questionnaire that did not carry out a learning process after implementing a system in the cloud

61%

Percentage of offices that responded to the State Comptroller's Office questionnaire that they do not have a master plan for computing or that their plan does not refer to cloud computing

99%

The vast majority of the offices that responded to the State Comptroller's Office questionnaire did not encounter multiple malfunctions in their cloud systems

Audit actions

From March to October 2020, the State Comptroller's Office examined aspects of government offices' use of the public cloud and preparations for the establishment of a central cloud. The audit was conducted at the Government ICT Authority in the Ministry of Digital Affairs, in the Procurement Administration in the Accountant General's Division of the Ministry of Finance and in the National Cyber Directorate in the Prime Minister's Office. Supplemental examinations were performed in the information systems divisions of several government ministries and support units, at the Federation of Local Authorities, in the Privacy Protection Authority in the Ministry of Justice and in

[1] According to the ICT Authority, 2020 activity at a glance.

[2] According to data from the Cyber Protection Unit (CPU) as of July 2020.

the Digital Transformation Administration in the ICT Division of the IDF. As part of the audit, the Office of the State Comptroller contacted 72 directors of main information systems divisions (hereinafter - MISDs) in government offices and their support units, and asked them to fill out a questionnaire on the use of public cloud services. Forty-five (about 62%) of the MISDs answered the questionnaire.

Key findings

Approved government plan for transition to cloud computing: The government plan for transition to cloud computing prepared by the ICT Authority was not presented to the Ministerial Committee as required by Government Decision 2097 of 2014, due to the dissolution of the committee in 2015 and its non re-establishment. It should be noted that the average annual utilization rate in 2018 of the existing local computing infrastructure resources in the government was 2%.

Nimbus Project: The Nimbus Project is a multi-year project that began in 2019 and is intended to provide a comprehensive solution to the issue of cloud services provision to government ministries. The project consists of four tiers that make up the central tender of the Government Procurement Administration. During 2020, tenders were published for the first tier (supply of cloud services) and the second tier (center of excellence in cloud computing) of the tender, and during February 2021, a tender was published for the third tier (modernization and migration services). A tender for the fourth tier (monitoring and optimization services) has not yet been published, and no estimated date has been set for its publication. The lack of a defined time frame for the project as a whole may lead to a prolongation of its implementation and a delay in the plan to migrate government offices to the cloud environment.

Mapping of the systems implemented in a cloud environment: As of the time of the audit, neither the ICT Authority nor any other government body had a complete and up-to-date mapping of all government systems that have already been implemented in the cloud. Such a mapping is required in order to obtain a complete and accurate picture of what is happening in the government offices and to verify that all government offices are operating in accordance with the guidelines of the ICT Authority regarding cloud computing.

Information security for work in the cloud: The director of the government's Cyber Protection Unit (hereinafter - CPU)[3] issued a specific directive which states that

[3] The CPU is a unit that operates within the framework of the Government ICT Authority in the Prime Minister's Office. The unit was established under Government Resolution 2443 "Promoting National Regulation and Government Leadership in Cyber Defense".

any system operating in the cloud environment requires the approval of the Advisory Committee on Transfer of Information and Computing Applications to the Public Cloud Environment, whether it is planned to move to the cloud or it is already operating in the cloud. Despite this directive, the responses of 42 offices to the questionnaire distributed by the State Comptroller's Office indicate that about ten systems operate in a cloud environment in these offices without the approval of the advisory committee. Operating such systems in a cloud environment without the committee examining whether this should be approved may lead to the realization of information security risks involved in operating these systems.

- **Information Security Guidelines for entities not controlled by the CPU:** Entities subject to sectoral guidelines by government ministries but not subject to CPU guidelines, such as communications, transportation and energy companies, independently manage the field of cyber protection in their computer systems, including cloud systems implementation, without a leading and supervising professional-regulatory entity - except for those that are defined as a critical state infrastructure and are closely supervised by the Cyber Directorate.

- **Control over the implementation of information security guidelines in the field of cloud environment:** There is no control over the implementation of the Cyber Directorate guidelines by the various entities. It also emerged that the Cyber Directorate does not have the authority to supervise and control the implementation of its guidelines in the area of cloud computing.

- **Requirements of the Advisory Committee for carrying out penetration tests into the cloud environment:** The Prime Minister's Office (hereinafter - PMO) is required to conduct penetration tests or risk surveys every 18 months for a government decision monitoring system uploaded to the cloud environment in December 2018. The audit found that the system had undergone penetration tests and a risk survey at the time of its establishment, but as of February 2021, no further penetration tests or additional risk surveys have been performed.

- **Contract without tender for the establishment of a system in a cloud environment:** In two of the three audited projects for the establishment of a cloud environment system, in the Ministry of Construction and Housing and in the Prime Minister's Office, it was decided to contract with a supplier to carry out the project without a tender process but rather on the basis that they were the sole supplier, based on the maximum price agreement signed between the supplier and the Government Procurement Administration. This is despite the fact that the maximum price agreement with the supplier did not apply to the supplier's cloud services, and a tender procedure could have been conducted.

- **Government lesson learning procedure:** No orderly government procedure has been formulated to draw lessons from the implementation of systems in the cloud environment. Such a procedure can help identify the barriers, difficulties and shortcomings that make it difficult for government ministries to implement systems in the cloud environment and help deal with them.

Publication of policies and guidelines: The Office of the State Comptroller welcomes the fact that the publications of the policies and guidelines of the ICT Authority and the CPU regarding cloud computing are updated in accordance with technological developments. It should be noted that in November 2020, the Procurement Administration issued a binding directive on "guidelines for the approval and control of cloud contracts". In addition, it should be noted that during the audit, the ICT Authority issued a directive in December 2020 on the subject of "approval, planning and control of cloud services."

Integration of additional entities in the Nimbus project: The State Comptroller's Office notes the integration of additional entities, such as institutional and financial entities, as well as the IDF, within the Nimbus project. The multiplicity of entities participating in the project enables the pooling of national resources and budgetary efficiency.

Key recommendations

- In order to facilitate the implementation of projects in a cloud environment in the future, both by the ministries independently and as part of the Nimbus project, it is proposed that the ICT Authority examine the full findings of this report and the conclusions drawn from them - the MISDs' answers to the questionnaire; the need to update its guidelines; the need to control the entities to ensure that they are implementing the guidelines; the establishment of a lesson-learning process, including by professional entities such as the Privacy Protection Authority; and the need for a uniform policy for all the entities that can serve as a basis for individual regulations.

- It is recommended that the Ministry of the Interior formulate a multi-year plan for the integration of municipalities in the Nimbus tender. As part of the plan preparation, it is worth considering the existence of a preliminary mechanism that will coordinate the ministry's guidelines for municipalities, including aspects of marketing, guidance and implementation, budgeting, etc. It is also proposed that the Ministry of the Interior and the National Cyber Directorate act as soon as possible to promote the establishment of a central Command and Control Center for handling cyber incidents in municipalities, in order to ensure functional continuity of municipalities.

- The Information System departments in government ministries must submit to the CPU a mapping of all the cloud systems in the ministries and update the advisory committee about the systems established in the cloud environment without its approval. The CPU must complete a mapping of all cloud systems in government offices. In this context, it is recommended that the Advisory Committee verify that in cloud ventures implemented prior to its establishment, the selected suppliers have adequate information security certifications. It is also recommended that the CPU apply control measures to ensure that the ministries implement its guidelines.

- In order to ensure the level of information security and cyber protection when implementing cloud transitions among entities subject to sectoral guidelines of government ministries, it is proposed that government ministries serving as regulators examine the need to establish dedicated cloud committees for entities subject to sectoral guidelines within such areas as transport, communications and energy. These committees will be able to ensure that the implementation of systems in the cloud meets the accepted standards in the areas of information security and cyber protection, as well as carry out controls on the implementation of cloud systems by these entities. Alternatively, it is recommended that government ministries consider the possibility of instructing their subordinate and supervised bodies to set up internal cloud committees that will report to the government ministry on the implementation of cloud systems.

- It is recommended that the Cyber Directorate shall consider the conduct of a periodic survey to examine the understanding and implementation of its guidelines on the implementation of cloud systems by government ministries and their support units, both to reduce the risk of not properly addressing the issue of information security when implementing a system in the cloud environment and to examine its effectiveness.

- It is recommended that internal auditors in all government ministries as well as the Municipalities Audit Division of the Ministry of the Interior consider the importance of the issue of cloud computing and the incorporation of this issue into audits in accordance with the methodologies used by these bodies for the selection of audit subjects.

- The State Comptroller's Office recommends that in light of the expected increase in contractual engagements regarding the transition to cloud environment, the Procurement Administration will ensure compliance with its guidelines regarding contractual engagements between ministries and suppliers for computer services in a cloud environment, and for this purpose it will examine the need to perform a comprehensive mapping of the contracts once every few years - including the dates of the contracts, their period of validity and cost.

Advantages and challenges of implementing cloud computing

Challenges of implementing cloud computing

- Adaptation of the organization structure to the cloud model
- Definition of clear responsibilities and boundaries
- Dependance on the cloud supplier
- Adaptation of the organization activity
- Compliance with the Information Security and privacy requirements
- Loss of capabilities in the organization
- Transfer process
- Subordination to foreign laws*

Main advantages of cloud computing

- Optimization of acquisition processes
- Specialization and leverage of scale advantages
- Purchase of services as needed
- Saving of capital costs
- Ability scope adjustment to the organization needs
- Agility
- Increasing business survivability against risks
- Focusing the organization on core activities
- Robustness

* When the service supplier is not Israeli, the data is subject to the laws of the supplier's country of incorporation or of the country hosting the servers.

Summary

Cloud technology allows easy and wide access to a common pool of computing resources. In recent years, the Israeli government has been working to transfer government ministries and their support units to the cloud computing model.

The situation that emerges in light of the findings of this report indicates various barriers that hinder or prevent the implementation of cloud computing systems in government ministries: various aspects that the ministries do not take into account in the implementation and may cause damage, ranging from pecuniary damage to image damage; the difficulty in controlling the ministries' implementation of the guidelines for the transition to a cloud computing environment, and the difficulty in controlling entities that are subject to the sectoral guidelines of the ministries but are not subject to the ICT Authority and the CPU guidelines; the lack of a comprehensive and approved framework for the transfer of government computer services to a cloud environment. In order to optimally implement the use of existing and future cloud computing systems, it is appropriate that the specified barriers and deficiencies and the given recommendations receive a comprehensive response, including as part of the Nimbus tender and the establishment of the Center of Excellence for Operation in the Cloud.