



Report of the State Comptroller of Israel – Cyber and  
Information Systems | November 2024

Systemic Audits

---

# Government Risk Management in the ICT





# Government Risk Management in the ICT

## Background

Digital technologies within government ministries are the core infrastructure for all governmental operations and a central means of managing and operating the ministries and providing service to the public. These ministries face various, including ICT<sup>1</sup> risks, impacting their operations and capacity to achieve their objectives.

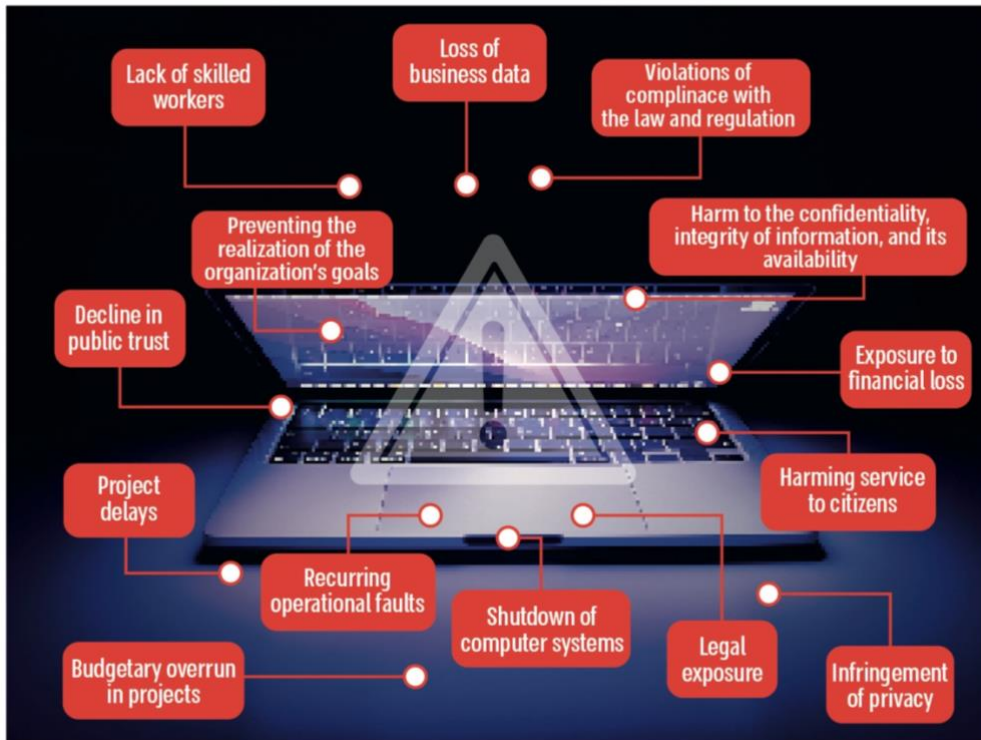
The necessity for ICT risk management in government is anchored in the government resolution from 2014<sup>2</sup>, the National Digital Agency guidelines<sup>3</sup>, the Financial and Economic Regulations (TAKAM) directives issued by the Accountant General at the Ministry of Finance<sup>4</sup>, and recognized international methodologies.

Implementing a structured and systematic approach for identifying ICT risk hotspots to which the ministry is exposed, assessing the implications and probabilities of these risks, preparing a comprehensive plan to mitigate or reduce them, and establishing a control system for early alerts regarding potential risk realization is essential to minimize the possible risks or their likelihood, and to prevent certain risks from materializing.

- 1 ICT risk – exposing ICT infrastructures, ICT processes or ICT projects to a failure event that could harm the organization and its goals, damage information, damage the level of service or lead to failure to meet mandatory standards.
- 2 Government Resolution 2097 (October 10, 2014).
- 3 As of 2023, 48 bodies – government ministries and auxiliary units – are guided by the National Digital Agency (government ministries).
- 4 Financial and Economic Regulations (TAKAM) directive 5.2.1 "Principles for managing operational risks at headquarters divisions in the Accountant General's Division and in the accounting departments of government ministries".



## Potential Damage Due to Realization of ICT Risks





**Key Figures**

**NIS 4.8 billion**

the government's ICT financial activity in 2022

**80%**

of government ICT workers are service providers (3,993 out of 5,308 in 2022), posing various risks to the recruitment and retention of personnel

**X**

the National Digital Agency did not formulate a government situation report of ICT risks nor reduce wide-ranging risks

**for about 2.5 years**

no Chief ICT Risk Manager has been appointed by the National Digital Agency (2021– 2023)

**about 65%**

of government ministries that reported in the "Itam"<sup>5</sup> system in 2022 (24 out of 37) noted that human capital is a key risk

**about 57%**

of government ministries that reported in the "Itam" system in 2022 (21 out of 37) noted that the budget is a key risk

**8 ministries**

of the 13 audited ministries (62%) had not appointed, as of July 2023, a ministry ICT risk manager

**8 ministries**

of the 13 audited ministries (62%) did not conduct a comprehensive organizational risk survey


5 A central information system for managing technological governance processes developed by the National Digital Agency.



---

---

## Audit Actions


 From November 2022 to August 2023, the State Comptroller's Office audited the management of ICT risks within the government. The audit examined the operations of the National Digital Agency for ICT risk management, the mapping of ICT risks at the national level, and the management of ICT risks across government ministries and auxiliary units. The audit was carried out in the National Digital Agency at the Ministry of Economy and Industry. Completion examinations were conducted in the DIT divisions (Digital and Information Technologies Divisions) across 13 ministries and auxiliary units supervised by the National Digital Agency. These included the Ministry of Finance, the Ministry of Justice, the Ministry of Education, the Ministry of Health, the Ministry of Foreign Affairs, the Ministry of Environmental Protection, the Ministry of Communications, the Ministry of Agriculture and Rural Development, the Ministry of Welfare and Social Affairs, the Enforcement and Collection Authority, the Population and Immigration Authority, the Ministry of Economy, and the Central Bureau of Statistics.

The audit focused on the ICT risk management processes regarding the development of central applications, the operation and maintenance of systems, facilities, and physical infrastructure, the procurement of equipment and software, and human capital, constituting most of the financial activities in this area (92%). Risk management concerning information and cyber security<sup>6</sup> was not examined.

---

## Key Findings



 **Appointment of a Chief ICT Risk Manager in the National Digital Agency** – from the end of 2020 until August 2023, the National Digital Agency did not appoint a Chief ICT Risk Manager, as required by the government resolution of 2014. This adversely affected the Agency's capacity to lead and guide DIT (data, information and technology) divisions within government ministries on ICT risk management and assist them in conducting ICT risk surveys and implementing risk mitigation plans. The absence of a Chief ICT Risk Manager also hindered the formulation of a comprehensive government situation report on ICT risks, deploying ICT risk management methodologies across government ministries, and promoting collaborative efforts to mitigate these risks.

---

<sup>6</sup> According to a government resolution from 2014, in all matters relating to cyber defense, the Chief ICT Risk Manager will be professionally guided by the Government Cyber Defense Unit (Yahav).



**Coordination of the Government Situation Report of ICT Risks and Initiating Lateral Activities to Reduce the Risks** – despite the 2014 government resolution assigning the National Digital Agency the responsibility for coordinating the government situation report of ICT risks and initiating lateral activities to reduce the risks, the following were found:

- The National Digital Agency did not form a cross-government situation report of ICT risks from 2021 to 2023, despite reports from several ministries in the "Itam" system during this period about their primary ICT risks. Since 2014, the ministry-wide ICT risk mapping was conducted only once, in 2019.
- The National Digital Agency has not monitored the evolution of ministry-wide risks within the government over the years nor tracked their levels and any changes.
- The National Digital Agency failed to mitigate lateral risks in 2022–2023 despite the obligations outlined in the government resolutions and receiving reports from ministries about the primary ICT risks they encountered.
- Knowledge retention within the National Digital Agency concerning managing ministry-wide ICT risks across the government is insufficient.

**Government Ministries' Reporting on Ministry-Lateral ICT Risks** – in formulating work plans, DIT divisions within government ministries were directed by the National Digital Agency to specify in the "Itam" system three to five primary risks that impact their capacity to meet their objectives. The following was found:

- In 2022 and 2023, about 20% of the 48 ministries guided by the National Digital Agency failed to report any ministry-wide ICT risks. In 2022, the ministries rate that did not report at all was 23% (11 ministries); In 2023, this rate decreased to 19% (9 ministries).
- Some government ministries submitted only partial reports, detailing one or two risks: In 2022, 40% of ministries reported partially (19 ministries). This increased in 2023, with 50% of ministries providing partial reports (24 ministries).

Consequently, in 2022 and 2023, 63% of ministries (30 ministries) and 69% of ministries (33 ministries), respectively, failed to comply fully with reporting requirements regarding ICT risks in the "Itam" system. The lack of comprehensive reporting by most ministries undermines the National Digital Agency's ability to create an accurate government situation report of ICT risks, analyze their implications, and devise ministry-wide actions and strategies for mitigation.

**The National Digital Agency Reporting on Ministry-Lateral Risks** – the National Digital Agency, responsible for the development of national digital services and technological infrastructures, was the only entity among the 48 ministries that did not utilize the "Itam" system for reporting ministry-wide ICT risks from 2021 to 2023. This



raises concern, particularly given the Agency's role as a benchmark for other government ministries.

**Reporting on Project-Level Risks** – an analysis of reporting practices between 2021 and 2023 raised that between two and 11 ministries out of 48 failed to report project-level risks each year.

**Assessing Government's ICT Risk Situation Report** – due to the National Digital Agency's failure to provide an updated situation report of ICT risks, the State Comptroller's Office conducted an analysis based on partial data from reports submitted by 37 government ministries through the "Itam" system, to identify ministry-lateral risks reported in 2022 and clarify the overall risk situation report:

- **Frequency of Reporting on Each Risk** – in 2022, the ICT risk most frequently reported by ministries was human capital, noted by 65% of ministries (24 out of 48). This encompasses issues such as inadequate standards, workforce shortages, insufficient employee skills, retention challenges, and recruitment difficulties. Additionally, budget-related risks were highlighted by over half of the ministries (57%, or 21 ministries), which include concerns such as the absence of an approved state budget and the partial funding of projects not included in the budget base. IT governance risks were noted by about 20% of ministries, indicating discrepancies between DIT division work plans and organizational business needs.
- **Risk Level Reporting** – the human capital risk was reported 22 times at high and very high-risk levels, describing a significant potential for damage with both high impact and likelihood of occurrence. The budget risk was reported 13 times at similar severity levels.

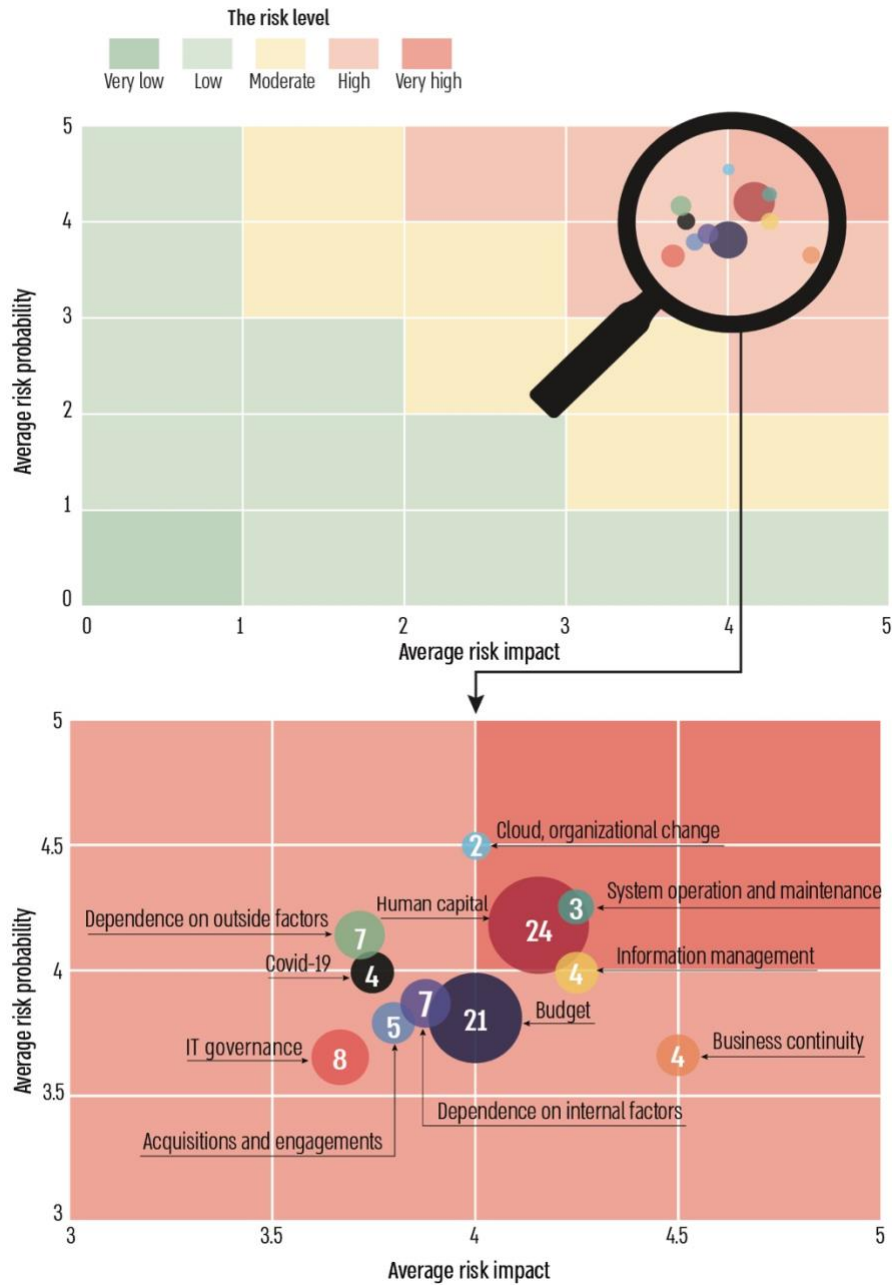
The State Comptroller's Office utilized a heat map to represent these risks visually. The color coding indicates risk levels: high risk is expressed in red, moderate risk in yellow and low risk in green. Each circle within the diagram represents a particular risk category; Its X-axis position illustrates the average impact of the risk, while the Y-axis indicates the average probability of risk occurrence. The size of each circle and the numbers contained within indicate the number of ministries that reported the respective risk.

The upper section of the heat map below displays the distribution of risks, while the lower section offers a focused view of high to very high-risks and the number of ministries reporting those risks.





## The Government Heat Map of ICT Risks, According to Reports in 2022 in the "Itam" System



According to the reports of the ministries in the "Itam" system, analyzed and processed by the Office of the State Comptroller.



The heat map indicates that all identified risks fall within a high to very high-risk category. This classification denotes the potential for significant damage with a high likelihood of occurrence. They are the most prominent risks, not only in the frequency of reports on them, but also in the high level of investigated risk. This heat map, derived from partial ministry reports, can guide the Agency and relevant government ministries in focusing their efforts on ICT risk mitigation, prioritize actions and resource allocation to address these risks.

**📌 Appointment of ICT Risk Managers in Ministries** – as of July 2023, eight out of the thirteen audited government ministries (62%) have not appointed an ICT risk manager, as required, including the Ministry of Education, the Population Authority, the Ministry of Agriculture, the Ministry of Communications, the Ministry of Foreign Affairs, the Ministry of Economy and Industry, the Ministry of Environmental Protection, and the Ministry of Welfare. Furthermore, the National Digital Agency lacked information regarding the appointment of these risk managers despite its mandate to maintain ongoing communication with ministries and receive updates on risk survey findings, material risks, and the progress of treatment plans.

**📌 Conducting a Comprehensive ICT Risk Survey at Ministries** – an examination conducted in 13 ministries regarding the execution of a comprehensive ICT risk survey, which maps the primary risks associated with the ministry's ICT activities and prioritizes their addressing, raised that:

- Three ministries – the Ministry of Justice, the Ministry of Health<sup>7</sup>, and the Ministry of Education, which are obligated by the National Digital Agency's guidelines to undertake a thorough organizational ICT risk survey due to their annual financial activities exceeding NIS 250 million<sup>8</sup>, have failed to conduct such surveys in the past four years. In 2022, the Ministry of Health's ICT financial activity was NIS 550 million, the Ministry of Justice's NIS 466 million, and the Ministry of Education's NIS 358 million.
- The Ministry of Justice – significant ICT risks were identified, including challenges related to cloud transition, personnel retention, and budget constraints. These risks affect the DIT Division's objectives, ranging from damage at the organizational unit level to the Ministry's overall goals. The Ministry of Justice has presented risk assemblage and specific mitigative measures to the State Comptroller's Office. However, these do not nullify a comprehensive ministry ICT risk survey as mandated by the National Digital Agency's guidelines nor facilitate informed decisions for addressing critical risk exposure.

7 The examination at the Ministry of Health does not encompass the Medical Centers Division.

8 According to data held by the National Digital Agency, "Overview of the government ICT activity 2022".



- The Ministry of Education – the Ministry of Education faced various significant ICT risks, including human capital, cloud transition, and the maintenance of outdated core systems. It has been noted that, despite the National Digital Agency's guidelines mandating a comprehensive organizational risk survey, the Ministry has not conducted such a survey in recent years. While some mitigation actions have been implemented to address specific known risks, this does not negate the necessity for a thorough ICT risk survey to identify and map additional material risks, along with a detailed mitigation plan to address them effectively.
  - The Ministry of Health – the Ministry of Health is encountering considerable risks and organizational challenges in ICT, including human capital, the transition to cloud infrastructure, outdated systems, budget constraints, and more. While the Ministry has developed a strategic plan to address these challenges, the plan lacks a detailed analysis of the associated risks and their significance, mitigation actions, and defined timelines for resolution. Furthermore, the Ministry has not performed a thorough organizational risk assessment in recent years, despite this being a requirement according to the National Digital Agency's guidelines.
  - Of the ten other audited ministries, whose annual ICT activities were less than NIS 250 million but still represent significant financial involvement, five ministries (50%) – including the Ministry of Welfare, the Ministry of Finance, the Ministry of Economy, the Ministry of Agriculture, and the Ministry of Communications – have not executed a comprehensive organizational ICT risk survey in recent years, despite recommendations from the National Digital Agency for all units to do so regardless of the financial scope of their activity.
  - As of August 2023, the National Digital Agency has not compiled a comprehensive mapping of government ministries and auxiliary units that have conducted thorough risk surveys, despite existing guidelines mandating ministries report findings, material risks, and progress of plans for addressing them to the Chief ICT Risk Manager.
- 📌 Risk Management in Projects** – it has been found that ICT risk management within the audited government ministries is often not conducted in alignment with the guidelines set forth by the National Digital Agency, nor systematically and continuously throughout the project life cycle. Additionally, it frequently lacks vital elements such as defining the level of risk and its implications, establishing a timeline for implementing mitigation actions, monitoring outcomes to determine whether the risk has been mitigated or expanded, and assessing the effectiveness of the mitigation measures.
- 📌 Risk Management in the National Digital Agency** – the National Digital Agency has not undertaken a comprehensive organizational ICT risk assessment as mandated by its guidelines, despite this being necessary due to its substantial financial engagement in



the ICT sector – at NIS 446 million annually – and its responsibility for managing critical core systems in the government's ICT sector.






**Formulation of a Policy and Methodology to Manage ICT Risks and Assisting to Implement Them** – over the years, the National Digital Agency has established a policy for managing ICT risks and implementing the corresponding methodology, which includes publishing guidelines and providing training for ministries. A National Digital Agency audit indicated that adopting these guidelines and methodology within the ministries is inadequate. To ensure optimal ICT risk management in government ministries, it is recommended that the Agency enhance its training and implementation efforts and explore additional actions necessary for the effective execution of ICT risk management processes in government offices.





**Establishment of the "Itam" System** – the National Digital Agency established the "Itam" system, a centralized information system for managing technological governance processes. This system incorporates a module for managing ICT risks, wherein a risk management methodology is applied. This methodology utilizes a central risk bank containing a list of typical and relevant ICT risks applicable to government ministries. The bank's objective is to efficiently, comprehensively, and promptly identify ICT risks, maintain consistency in risk mapping, and facilitate cross-cutting analyses of ICT risks across government ministries.

---

## Key Recommendations

-  The National Digital Agency should map and analyze organization-wide ICT risks, update the cross-government ICT risk map, and continuously monitor risk levels. It is recommended that this map be integrated into the annual government-lateral situation picture regarding ICT activities. Furthermore, the National Digital Agency should initiate organization-wide measures to mitigate these risks and report its actions for risk mitigation to the government ministries.
-  For the National Digital Agency to comply with the government resolution, formulate a comprehensive picture of all ICT risks, and mitigate them, it should ensure all government ministries report in the "Itam" system, including ministry-lateral and project-specific risks. This requires refining and clarifying reporting guidelines to achieve a complete situational report.
-  Ministries that have not appointed a ministry ICT risk manager should prioritize the appointment of this role promptly. The National Digital Agency should also supervise this process to confirm that all ministries appoint such positions.



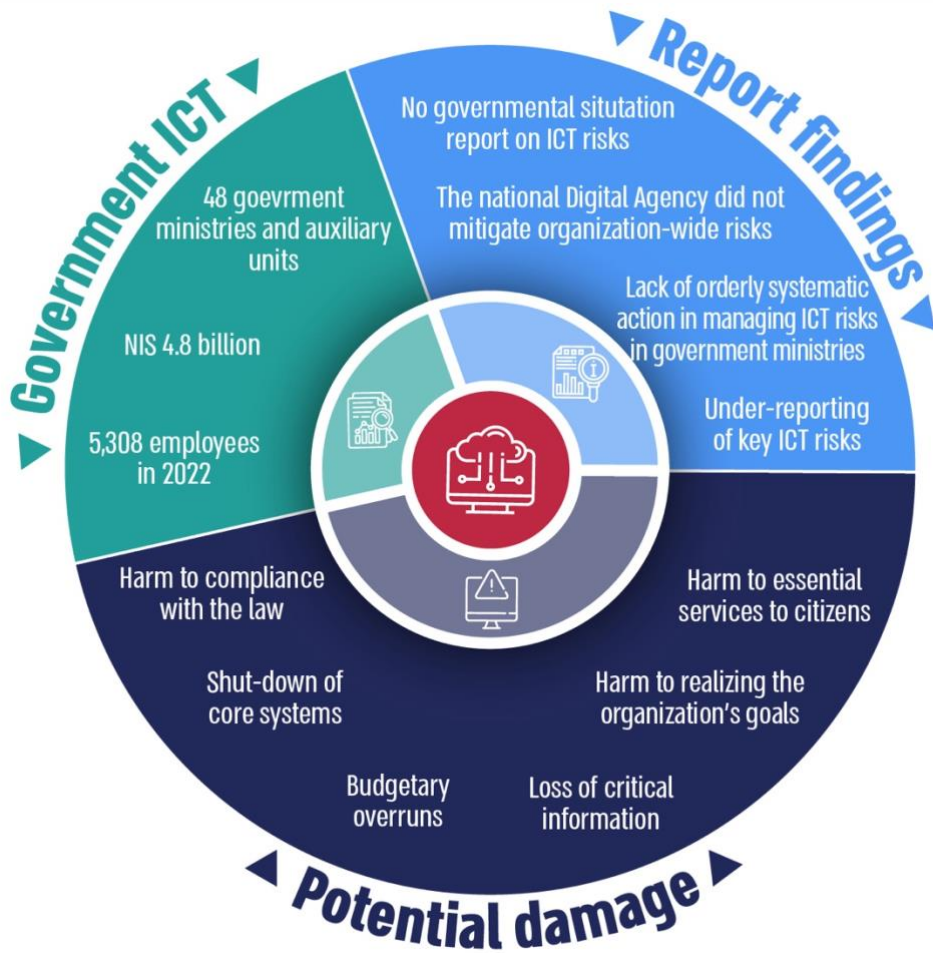
-  Ministry ICT risk managers should maintain a consistent risk management routine, including a work plan for risk assessments and the development of an annual plan for managing ICT risks.
-  It is recommended that the National Digital Agency monitor the ministries' execution of risk assessments and adherence to established mitigation plans. Additionally, the Agency should consider lowering the threshold requiring organizational ICT risk surveys for ministries with annual ICT financial activities below NIS 250 million.
-  The National Digital Agency should map and analyze systemic risks affecting all facets of technology and digital transformation within the government, particularly evaluating risks linked to the non-adoption of new technologies<sup>9</sup>, and formulate a comprehensive long-term management policy. This should include identifying organization-wide ICT risks raised by government ministries.
-  Finally, the National Digital Agency should enhance its initiatives regarding implementing risk management methodologies within the ministries.

---

9 RONI-Risk Of Not Investing



## Government Risk Management in the ICT – Summary Chart





---

---

## Summary

Digital transformation and its integration into government work processes present opportunities for improving efficiency and enhancing public services, along with new challenges and risks. It is, therefore, essential to manage ICT risks within the government systematically and methodically.

This report identifies significant gaps in ICT risk management in the government, including the absence of a centralized situation report of ICT risks, inadequate actions taken by the National Digital Agency to mitigate organization-wide risks, insufficient reporting from government ministries on critical ICT risks requiring attention, and the lack of a centralized, systematic approach to managing ICT risks across ministries, including both inter-ministerial risk management and risk management within ICT projects.

The National Digital Agency should consider the findings of this report and the accompanying government heat map of ICT risks to prioritize relevant efforts. This will ensure that risk management in this complex and dynamic field is conducted effectively, allowing for proactive preparation for challenges and responsive adaptation to changes in the environment of governmental activity.

