



Report of the State comptroller of Israel | January 2024

Systemic Topics

Supply Chain Cyber Risk Management in the ICT Sector



Supply Chain Cyber Risk Management in the ICT Sector

Background

The supply chain encompasses all the resources and processes of suppliers, customers, and contractors necessary to provide the organization with a product or service. Cyber-attacks carried out through the supply chain may harm one of the organization's suppliers, exploiting the organization trust in its suppliers to gain access to the organization.

In recent years, there has been a significant increase in the number and intensity of cyber-attacks on organizations, and today, cyber-attacks through their supply chain pose one of the most severe threats to the entire economy. Here are a few examples of such attacks in 2020–2022: In November 2020, a significant scope of highly confidential data, including terabytes, relating to customers of a large insurance company, was leaked. This data breach included information from thousands of civil servant files due to exploiting vulnerabilities in the insurance company's systems. In October 2021, sensitive information from one million profiles on a gay community dating site was leaked through an attack on a supplier providing hosting and storage services to the dating site as well as to other sites.

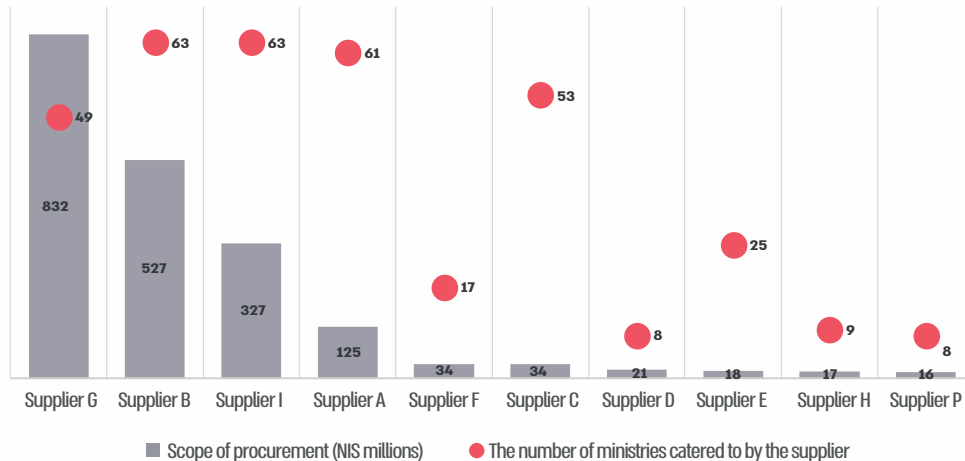
Government ministries and critical state infrastructure entities¹ (CSI entities) must address the supply chain risks by incorporating cyber protection requirements into their tender and contracting procedures.

Harming suppliers who cater to multiple government ministries or CSI entities can be particularly severe, as it could disrupt the economy's functional continuity or leak susceptible information. According to this audit, government ministries have 18 key suppliers in the ICT (Information Communication Technology) and cyber domain – of these, five suppliers provide services to over 49 ministries, and three suppliers provide services at over NIS 327 million, as presented in the chart below:

¹ Organizations defined in the Regulation of Security for Public Entities Law, 1998, as critical state infrastructures.



Suppliers in the ICT and Cyber Sector Catering to Numerous Ministries (financial scope in millions of NIS)



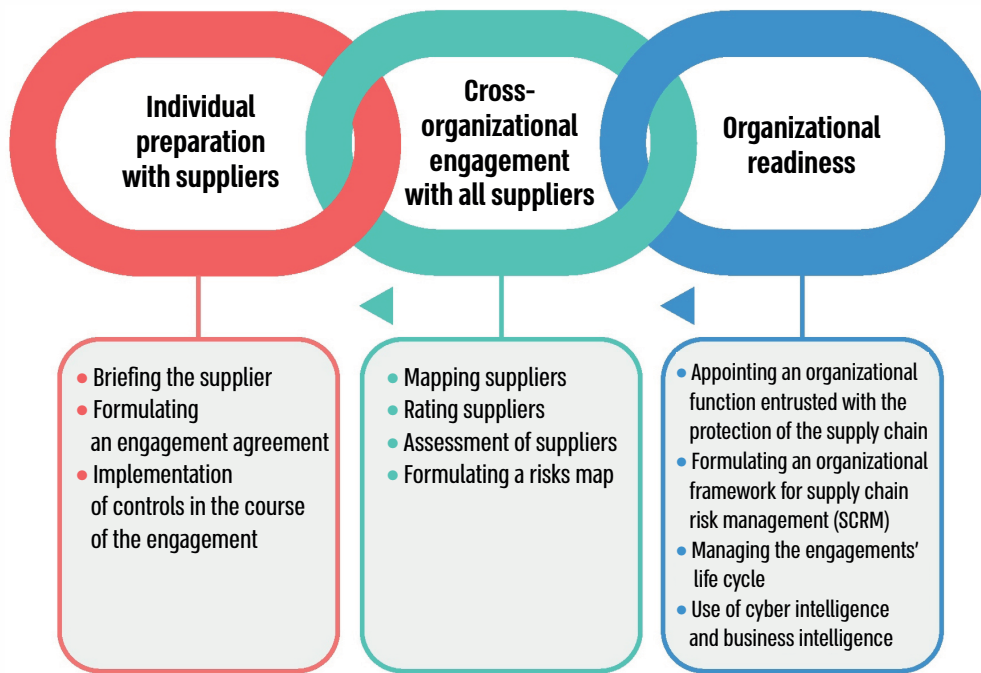
According to the government procurement system data, processed by the Office of the State Comptroller.

The National Cyber Directorate (the Cyber Directorate or the Directorate), acknowledged the risk posed by cyber-attacks targeting the supply chain and, in 2018, introduced a dedicated methodology for the economy (the Supply Chain Methodology), which is published on the Cyber Directorate website² as a recommendation for the economy. Furthermore, the Cyber Directorate released a dedicated guideline for critical state infrastructure entities based on the methodology above. The Government Cyber Defense Unit (YAHAV), responsible for providing guidance and professional advice on cyber protection to all government ministries and auxiliary units, also published, in November 2019, a dedicated guideline focusing on the supply chain based on the Cyber Directorate's methodology. The Supply Chain Methodology underwent an update in December 2022. Subsequently, in 2023, the guidelines provided to the CSI entities and government ministries were duly revised according to the updated methodology.

² https://www.gov.il/he/departments/guides/supply_chain_guide



The Key Stages of the Cyber Directorate's Supply Chain Methodology



Source: The Cyber Directorate.



Key Figures

The following figures are derived from the information gathered through the responses of 44 government ministries and critical state infrastructure (CSI) entities to a State Comptroller's Office questionnaire.

30%

of the government ministries and the CSI entities reported that in the last two years, they experienced a cyber incident that originated in the supply chain

86%

of the government ministries and the CSI entities defined a cyber incident through an attack on the supply chain as a threat of attribution to the organization

55%

of the government ministries and the CSI entities do not operate according to the Cyber Directorate's Supply Chain Methodology

41%

of the government ministries and the CSI entities have not performed cyber audits of their critical suppliers in the last three years (2020–2022)

57%

of the government ministries' ICT and cyber engagements in 2021, were performed through key tenders – do not include a requirement to implement the Supply Chain Methodology

84

cyber incidents in website hosting and storing companies in 2021–2022

43%

of the government ministries and the CSI entities do not involve the Cyber Protection Officer in the procurement processes


not one

of the 13 critical suppliers that provide services to several CSI entities were not certified by accreditation bodies³

³ Suppliers classified as critical by the organization (Suppliers rated A) are required, according to the Supply Chain Methodology, to complete, together with an external examiner certified by the Cyber Directorate, a supplier questionnaire that checks their level of protection. The questionnaire is forwarded to an accreditation entity, and it checks the reports submitted in the questionnaire and the evidence attached to it. The certification entity can ratify the report and issue the supplier a certification that will be valid for two years or not ratify the report and ask it to rectify deficiencies.



Audit Actions

 From February 2022 to May 2023, the State Comptroller's Office audited the supply chain cyber risk management within the ICT. The audit was carried out at the Prime Minister's Office – the National Cyber Directorate and the Security, Emergency, and Cyber Division; At the National Digital Agency – the Government Cyber Defense Unit (YAHAV) as well as the Available Government Unit; At the Ministry of Finance – the Procurement Administration and the Security, Emergency, and Cyber Division. Completion examinations were carried out in several government ministries and critical state infrastructure (CSI) entities. In all organizations, the audit examined unclassified networks.

As a part of this audit, the State Comptroller's Office circulated a questionnaire among 58 government ministries and CSI entities to assess their coping with the risk of cyber-attacks on the supply chain. This questionnaire was based, among other things, on various issues and gaps identified during meetings conducted between the audit team and the government ministries and CSI entities, and its primary objective was to provide a comprehensive overview of how government ministries and CSI entities handle this critical matter. 44 government ministries and CSI entities responded to the questionnaire (31 government ministries and 13 CSI entities).



Below is a list of government ministries and critical state infrastructure entities to which the questionnaire was distributed (the government ministries and CSI entities that responded to the questionnaire are highlighted): **Entity 1, the Planning Administration, Entity 2, the Ministry of Energy and Infrastructure, the Israel Meteorological Service, Entity 5, the Chief Rabbinate of Israel, the Ministry of Construction and Housing**, the Ministry of Strategic Affairs and Public Diplomacy, **the Ministry of Welfare and Social Affairs, the Water Authority**, the Courts Administration, **the Agricultural Research Administration**, the Consumer Protection and Fair Trade Authority, **the Competition Authority, Entity 11, the Civil Service Commission, Entity 15, Entity 50, Entity 16, Entity 51, the Ministry of Social Equality**, the Government Advertising Bureau, **the Ministry of Agriculture and Rural Development, the Ministry of Tourism**, Entity 52, **Entity 19, Entity 20, Nativ (the Prime Minister's Office), Entity 21, the Prime Minister's Office**, the Ministry of Innovation, Science and Technology, **the Enforcement and Collection Authority, the Ministry of National Security, the Geological Survey of Israel, the Ministry of Economy and Industry, the National Fire and Rescue Authority, the Ministry of Religious Services, the Ministry of Aliyah and Integration**, the Ministry of Transport and Road Safety, **the Ministry of Culture and Sports**, the Ministry of Communications, **Entity 38, the Ministry of Health**, Entity 53, **Entity 39**,



the Administration for Rural Residential Education and Youth Aliyah, the Ministry of Labor, the Ministry of Environmental Protection, Entity 54, the Rabbinical Courts Administration, the Israel Land Authority, the Ministry of Interior, Entity 43, Entity 45, the Ministry of Foreign Affairs, Entity 55, the Ministry of Justice.

This report focuses on the supply chain risk management of government ministries and CSI entities, bound to adhere to the YAHAV and the Cyber Directorate guidelines, respectively, which, during the audit period, were based on version 1.3 of the Supply Chain Methodology. In December 2022, the methodology was revised to version 1.4, among other things, to rectify some of the gaps highlighted in this audit report.

Key Findings

-  **Implementing the Cyber Directorate's Supply Chain Methodology in all Organizations** – out of the 44 government ministries and critical state infrastructure (CSI) entities that responded to the questionnaire, 24 (55%) do not adhere to the Cyber Directorate's Supply Chain Methodology. Consequently, a significant rate of the organizations' suppliers is not subjected to standardized examination and controls defined by the Cyber Directorate. Additionally, all sectoral cyber units experienced challenges in implementing the methodology, including high certification costs, the lengthy time it requires, difficulties working with international suppliers, and the complexity of incorporating cyber protection requirements into existing tenders.
-  **Addressing the Gaps in the Supply Chain Methodology** – in December 2022, the Cyber Directorate updated version (1.4) of the Supply Chain Methodology to the public. However, this current methodology fails to address specific critical gaps that were raised during the Cyber Directorate's Steering Committee meeting on the supply chain in January 2022, including the inherent difficulty of compelling the examined suppliers to fully comply with the existing controls outlined in the supplier questionnaire, without the option of compensatory measures for specific requirements or evidence of compliance with parallel standards, as well as failure to provide a solution for working with international suppliers. For instance, a proposal was made to examine the architecture of various industrial controllers' components supplied by a specific company to various sectors of the Israeli economy, and based on these insights, the Cyber Directorate, as a



cyber regulatory body, will lead the discourse concerning security requirements that the company must meet.

Supply Chain Risk Management in Key Tenders – although 57% of government procurement in the ICT and cyber sector (with an annual financial volume of approximately NIS 1.4 billion) are conducted through key tenders, the Procurement Administration does not obligate the suppliers it engages to comply with the Cyber Directorate's Supply Chain Methodology. Moreover, the Cyber Directorate and the Government Cyber Defense Unit (YAHAV), which routinely guides CSI entities and government ministries, are not regularly involved in formulating requirements for these tenders.

Mapping Suppliers with Extensive Impact on the Economy – based on the State Comptroller Office questionnaire, 18 primary ICT and cyber suppliers offer services to multiple government ministries and CSI entities. Five suppliers cater to over 49 government ministries and CSI entities, while three provide services at over NIS 327 million annually. However, it was found that the Cyber Directorate and YAHAV lack a standardized list of critical suppliers serving government ministries and CSI entities, the winners of key tenders, and the organizations contracted in each engagement. Furthermore, proactive intelligence collection is not carried out to detect potential threats to these suppliers. Consequently, regulatory bodies cannot assess the level of exposure of the ministries and CSI entities to these suppliers and take proactive actions with suppliers to increase their level of protection.

Integration, IT, and Website Storing and Hosting Suppliers – the Cyber Directorate is not authorized to enforce the Supply Chain Methodology on website storing and hosting companies and integration and IT companies that serve multiple organizations within the economy. Furthermore, several recurring cyber incidents have been detected within these companies (84 cyber incidents experienced by storage companies in 2021 and 2022), placing numerous organizations in the economy at a significant risk.

Certification of Critical Suppliers (rated A) – none of the 13 critical suppliers providing services to various CSI entities have undergone the certification procedure by certification bodies, despite the Cyber Directorate's guidance requiring that 30% of the essential suppliers of the CSI entities should be certified by the conclusion of the fourth quarter of 2022. Among the reasons for the low certification rate is the extensive duration of the certification process (over 9 months), which fails to align with the urgent business needs of organizations, and the unwillingness of relevant parties (the suppliers, ministries, CSI entities, and the Cyber Directorate) to bear the costs associated with the certification.

Auditing of Critical Suppliers (rated A) – the Cyber Directorate, YAHAV, and the Procurement Administration do not audit critical suppliers providing services to numerous




ministries and CSI entities nor of suppliers winning key tenders (even though the rate of engagement with them is at about 57% of all governmental ministry engagements, of about NIS 1.4 billion). Furthermore, 14 (41%) of the 34 government ministries and CSI entities that answered the questionnaire did not audit their critical suppliers.

🗨️ Reports by Suppliers on Cyber Incidents – 13 (30%) of the 44 government ministries and CSI entities had experienced a cyber incident originating in the supply chain within the past two years (2021–2022). However, 8 (62%) of these government ministries and CSI entities were not informed directly by the suppliers but rather from external sources (such as the Cyber Directorate or media outlets). Furthermore, the Procurement Administration included in key tenders published after 2021 an obligation for suppliers to promptly report any cyber incidents to the Administration itself, with the introduction of the Information Security Appendix. However, suppliers are not obligated to report these incidents to the Cyber Directorate. Since the Procurement Administration lacks a dedicated call center for receiving inquiries about cyber incidents and analyzing the received information – unlike the Cyber Directorate – there is a risk of inadequate incident management or delayed responses, jeopardizing the ministries.

🗨️ The Information Security Appendix – both the draft of Appendix G of TAKAM (Regulation, Finance, and Economy Directives) Directive No. 7.3.1 issued by the Procurement Administration and Directive 5.19 published by YAHAV instruct the ministries to add to their tender engagements with the supplier an Information Security Appendix. It was found that both directives are inconsistent, as each directive refers to an information security appendix with provisions on different topics. Consequently, the ministries will find it hard to determine which appendix they should incorporate into their tenders. The complexity arising from different directives and appendices is exacerbated by the fact that each directive targets different audiences (the TAKAM directive is tailored for procurement officials, while the YAHAV directive is intended for cyber protection officers), and in some organizations, the cyber protection officers are not involved in the procurement processes.

🗨️ Involvement of the Organization's Cyber Protection Officials in the Procurement Processes – 19 (43%) of the 44 government ministries and CSI entities that responded to the questionnaire stated that the cyber protection officer or the supply chain officer is not involved in the ICT and cyber procurement processes in the organization. It was further found that in 14 (40%) of the 35 government ministries and CSI entities that responded to the questionnaire, the cyber protection official is not involved in the termination process of the supplier's contract and does not verify whether the supplier fulfills its termination obligations (such as the deletion of information, returning of resources, disconnection of remote access and more). These shortcomings raise concerns over the failure to address information security in ICT and cyber engagements, consequently exposing government ministries and CSI entities to information security risks throughout the engagement period.



 **Coordination Among Regulatory Bodies Operating in Supply Chains** – it was found that the regulatory bodies (the Cyber Directorate, YAHAV, the Israel Security Agency, the Director of Security of the Defense Establishment, the Privacy Protection Authority, and sectoral cyber units) and the Procurement Administration have established different requirements concerning the supply chain without proper coordination and integration of these requirements. This state of affairs contradicts Government Resolution 2118 of October 2014 to minimize regulatory burdens. Additionally, collaborative efforts between regulatory bodies to explore resource sharing, developing joint systems, and exchanging information and knowledge within the field have not been carried out.





The State Comptroller Office commends the six ministries for implementing the methodology to a high level (score of 74 and above): Entity 31, Entity 22, Entity 18, Entity 28, Entity 8, and Entity 34.

Although the Directorate does not have authority over website storing and hosting companies, the National Cyber Emergency Response Team (CERT), through the Interfaces Center, established required standards for hosting companies, which are the "soft underbelly" of the ICT sector. By the audit end date in May 2023, 13 companies have voluntarily expressed their consent to the process, and implementation is scheduled to begin in 2023, subject to completion of the internal process within the Directorate.

The State Comptroller's Office commends Entity 20, Entity 44, Entity 35 (in the classified network), Entity 46, and Entity 47 for investing dedicated resources in supply chain risk management beyond what is required under the Supply Chain Methodology.

Key Recommendations

-  It is recommended that the Cyber Directorate and the Government Cyber Defense Unit (YAHAV), responsible for formulating the Supply Chain Methodology and the derived guidelines and for monitoring their implementation in practice, ongoing monitor the implementation level of version 1.4 of the methodology and cooperate with the bodies to diminish the gaps if any arise. It is further recommended that the Cyber Directorate provide specific guidance for implementing version 1.4 of the Supply Chain Methodology to the relevant cyber units and monitor the implementation of the methodology to ensure that the gaps found in the implementation of version 1.3 are addressed.
-  It is recommended that the Procurement Administration include in its tenders the regulatory bodies' requirements in cyber, particularly the requirement to implement version 1.4 of the Supply Chain Methodology, and if it believes that there is difficulty in



implementing these requirements as formulated or if there is a better alternative, it is recommended that it discuss this matter with the regulatory bodies and obtain their consent for alternative requirements to be implemented.



It is recommended that the regulatory bodies in cyber (the Cyber Directorate, YAHAV) receive the mapping of critical suppliers from the entities guided by them and the mapping of suppliers who won ICT and cyber key tenders from the Procurement Administration and update these lists periodically. Thus, the regulatory bodies can obtain a comprehensive picture of the ministries' exposure level to these suppliers and, if necessary, enhance their defense level. It is further recommended that the regulatory bodies in the cyber domain transfer the list of critical suppliers to the Intelligence and Guidance Center at the Cyber Directorate; thus, it will include these suppliers in its priority intelligence requirements and alert the ministries in the event of concern about any potential harm to them.



It is recommended that the Cyber Directorate examine the regulation of entities such as IT companies, integration companies, and website hosting companies, including their ability to implement the Supply Chain Methodology, whether through regulation or alternative means. Furthermore, it is recommended that the Cyber Directorate examine this issue in coordination with relevant regulatory bodies in information security and cyber protection, such as the Director of Security of the Defense System and the Privacy Protection Authority.



It is recommended that the cyber regulatory bodies (the Cyber Directorate, YAHAV) reduce the costs incurred by organizations that seek to add a requirement for compliance with the Supply Chain Methodology to suppliers providing services to CSI entities and various ministries. This can be achieved, for example, through joint certification by multiple entities and through the assistance of a certified supplier auditor appointed by the regulatory body to assess the supplier's compliance with the required controls in the methodology.



It is recommended that the Procurement Administration, the Cyber Directorate, and YAHAV define together the types of key tenders and types of services in the ICT and cyber that would benefit from auditing by a regulatory body in the cyber protection, focusing on key tenders where the level of risk and sensitivity is high. They should also cooperate with the ordering party to incorporate a provision in the tender that permits them to conduct audits. It is further recommended that government ministries and CSI entities that have not audited their critical suppliers do so and follow up on rectifying the deficiencies identified with the suppliers.



It is recommended that a mandatory guideline be added to key tenders in the ICT and cyber, as well as the final version of Appendix G of the TAKAM Directive No. 7.3.1, requiring suppliers to report both to the Cyber Directorate and to the ordering party about any concern regarding information security and cyber incidents they experience. Moreover, it is recommended that cyber regulatory bodies and entities guiding themselves and using key tenders provide the Procurement Administration with a timely summary of the incidents



experienced by suppliers who won any key tender, along with how they were dealt with and provide recommendations for future collaboration with the supplier.



It is recommended that the Procurement Administration collaborate with the regulatory bodies in the information security and cyber (the Israel Security Agency, the Director of Security of the Defense Establishment, the Cyber Directorate, YAHAV, and the Privacy Protection Authority) to add an information security appendix to all engagement documents or guidelines that will require every organization to add an information security appendix according to the guidelines of the relevant regulatory body guiding it in the information security and cyber protection.



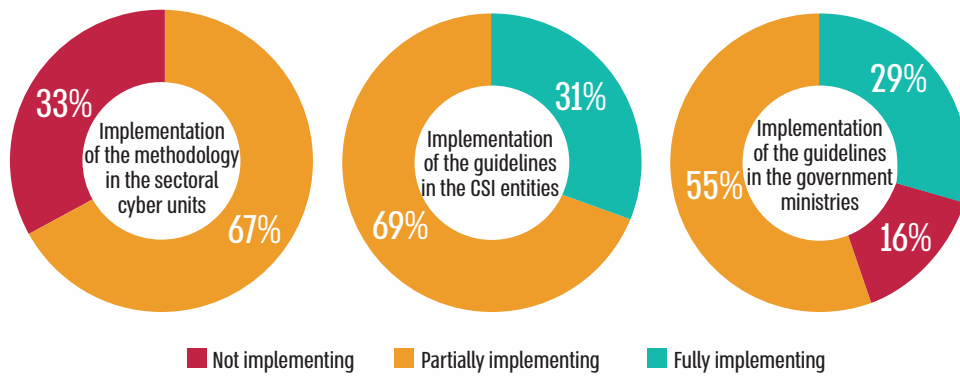
It is recommended that the Accountant General Division in the Ministry of Finance update the relevant TAKAM instructions, thus obligating the ministries to involve either the Cyber Protection Officer or the Supply Chain Officer in the ICT and cyber procurement processes including in the termination of contractual agreements with suppliers, and to receive from them information security requirements to provide comprehensive and adequate response to cyber risks that may be associated with the tender process.



It is recommended that the Cyber Directorate convene all the regulatory bodies responsible for the supply chain (the Cyber Directorate, YAHAV, the Israel Security Agency, the Director of Security of the Defense Establishment, the Privacy Protection Authority, sectoral cyber units), as well as the Procurement Administration, to integrate different methodologies, discuss common topics such as international standardization, consider joint resource allocation, creating shared systems, and establishing a professional forum on the supply chain.



Implementation of the Methodology and Guidelines in the Organizations Examined



According to answers to the questionnaire sent by the Office of the State Comptroller, processed by the Office of the State Comptroller.

Implementation of the Methodology in the Critical State Infrastructure Entities

[illegible]

According to answers to the questionnaire sent by the Office of the State Comptroller, processed by the Office of the State Comptroller.



Summary

The threat of attribution of a cyber-attack through the supply chain is one of the most concerning threats to organizations within the economy. 86% of the 43 organizations surveyed identified an attack through the supply chain as their primary threat of attribution, and about 30% of the organizations answered that they experienced a cyber incident originating from the supply chain within the past two years (2021–2022). The challenge in addressing this threat is that the required protection of the supplier is ostensibly outside of the organization's purview.

This report indicates that certain suppliers provide services to numerous government ministries and critical state infrastructure (CSI) entities, and therefore, harming them may result in widespread disruptions to the government's and the economy's functionality.

The Cyber Directorate, the regulatory authority responsible for enhancing cyber protection in the economy, introduced a methodology in 2018 for managing the risks associated with the supply chain. The findings in this report, based on the examination of the methodology's implementation across government ministries, auxiliary units, CSI entities, and sectoral cyber units, indicate specific gaps in addressing this issue, as outlined in detail below:

1. About six years after the formulation of the Supply Chain Methodology by the Cyber Directorate, it has not yet been integrated into the economy, and specific organizations assert that the implementation of this methodology is unfeasible. A survey among government ministries and CSI entities raised that 55% of respondents do not adhere to the supply chain methodology. Consequently, numerous suppliers associated with these organizations are not subject to uniform examination under the guidelines set by the Cyber Directorate.
2. Significant gaps in the implementation of the methodology have been identified, which have yet to be addressed by the Cyber Directorate, such as the inability to apply requirements to international suppliers, the high costs of certification, and its lengthy process that does not align adequately with the business needs of organizations.
3. The report found that government ministries rely on 18 key suppliers in the ICT and cyber sectors who service multiple organizations. Five suppliers cater to over 49 ministries, while three provide services at over NIS 327 million annually. These suppliers are not properly certified, and some are not subject to supply chain controls – which threatens the organizations they serve. Furthermore, cyber regulatory bodies have failed to adequately map and promote these suppliers' certifications.
4. None of the regulatory cyber bodies guides the Procurement Administration. Additionally, in key tenders, the Procurement Administration does not require suppliers with whom it contracts to adhere to the Supply Chain Methodology or to additional security



requirements that the regulatory bodies demand from the ministries, even though these contracts represent an average of about 57% of all contracts in the ICT and cyber. Furthermore, no audit is conducted to assess the level of cyber protection offered by suppliers who have won key tenders.

5. The cyber protection officer in government ministries and CSI entities is not involved in the ICT and cyber procurement processes within the organization and does not participate in the termination of contracts with suppliers to ensure the fulfillment of contractual obligations by the supplier (data deletion, returning of resources, disconnection of remote access and more).
6. Government ministries and CSI entities experienced cyber incidents in the supply chain within the past two years (2021–2022). However, updates regarding these incidents were not received directly from the suppliers but from other entities, such as the Cyber Directorate or media outlets. Furthermore, the Procurement Administration does not obligate suppliers who have won key tenders to report cyber incidents to the Cyber Directorate.
7. Cyber Regulatory bodies (the Cyber Directorate, the Government Cyber Defense Unit (YAHAV), the Israel Security Agency, the Director of Security of the Defense Establishment, the Privacy Protection Authority, the sectoral cyber units) and the Procurement Administration have established different requirements concerning the supply chain without proper coordination and integration of these requirements, creating a regulatory burden on both organizations and suppliers.

The above gaps necessitate a thorough assessment of the current methodology's response and its implementation, as findings indicate a genuine risk to CSI entities, government offices, and sectors stemming from the ICT supply chain. It is crucial that the Cyber Directorate and cyber regulatory bodies, as well as the Procurement Administration, carry out this situational assessment. Simultaneously, all government ministries and CSI entities should fulfill their respective responsibilities in rectifying the deficiencies outlined in this report, thereby ensuring enhanced protection for the suppliers and the overall economy.

During the audit, the National Cyber Directorate and YAHAV revised their guidelines for the ministries and CSI entities, among other things, to address the gaps identified in this report. Therefore, the Cyber Directorate and YAHAV should monitor the assimilation of the latest methodology and its implementation in practice over the upcoming year.

