

SUPPLY CHAIN

when all links are **strong**,
your organization is protected



Cyber Israel

Prime Minister's Office
National Cyber Directorate



Cyber Israel

Prime Minister's Office
National Cyber Directorate

Regulating Supply Chain Cyber Defense in the Israeli Economy

APRIL 2021

This document was written by the Israeli National Cyber Directorate as a public service, within the framework of the Directorate's commitment to improve the capabilities of the organizations in the economy to respond to cyber threats.

This document may be used by Organizations free of charge, provided that the State of Israel's lawful rights are protected. It should not be considered a substitute for obtaining individual advice on customizing the recommendations herein to suit the specific organization.

This document is written in the masculine gender solely for the sake of convenience.

Comments on the contents of this document may be forwarded by e-mail to

tora@cyber.gov.il.



Table of Contents

Introduction	3
Scope.....	8
Deliverables of initiative	11
Description of the process from the organization's perspective	13
Description of the process from the supplier's perspective	17
Description of the regulation process.....	20
Appendix A - The process from the organization's perspective	22
Appendix B - Supplier Questionnaire	38
Appendix C - Supply Chain Module	41
Appendix D - Regulation model	44
Appendix E - Sample agreement	57



Cyber Israel

Prime Minister's Office
National Cyber Directorate

INTRODUCTION

1





- 1 In the Israeli economy, organizations both large and small invest in cyber security in order to minimize the risk of cyber-attacks that could cause them substantial financial losses and result in the theft of trade secrets, harm to reputations, disruption of functional continuity, etc. Some organizations are aware that they could be similarly compromised through their supply chain, if their data stored by a supplier is stolen and their organization's system is breached via access authorizations granted to the supplier, etc.

- A BOMGAR survey found that only 35% of data-security experts in global organizations knew with certainty how many suppliers had access authorizations to their organization's systems.
- That same survey found that on average, suppliers access an organization's network 89 times a week.
- Another survey finding was that 69% of the respondents believed that their organization had suffered a data-security incident over the past year as a result of lenient access authorizations to the organization's systems.
- In 2016, organizations that experienced a data-security incident originating from their supply chain were forced to spend on average about USD 10 million on responding to and handling the incident (source: CSO Online).
- About 63% of all cyber-attacks are a direct or indirect result of vulnerabilities exploited in the supply chain (source: Soho Systems).

- 2 The Israeli National Cyber Directorate (hereinafter: "the Directorate") has written and publicized national guidelines entitled "Cyber Defense Methodology for Organizations" with the aim of helping organizations manage their cyber risks.¹ This methodology defines, inter alia, an organization's need to defend itself against attacks through its supply chain. However, organizations are singularly limited in their ability to control the cyber defense activities of their suppliers. Many organizations lack the professional knowledge to formulate their own requirements from their suppliers and do not have the resources to verify the extent of their suppliers' compliance with the cyber defense requirements. As a result, the level of cyber defense is significantly lower with many suppliers than the level of defense that the organization demands of itself. As evidence of this, many cyber-attacks against organizations are carried out through their supply chain.

¹ https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_418_A4.pdf (in Hebrew)



3 The Directorate met with suppliers, customers, regulatory authorities and consultants throughout 2018 and became aware of the following shortcomings and inadequacies in the economy:

- There is no standardization or common language between organizations in the economy and their suppliers. The economy is basically characterized by organizations that do not conduct cyber defense activities in relation to their supply chains and organizations that have developed their own questionnaires (which, for the most part, are not customized according to the various types of risks). This creates complications for organizations and the need to invest resources in developing and updating their questionnaires.
- Organizations are having a difficult time managing the process of distributing the questionnaire, answering suppliers' questions and analyzing the findings. They are required to distribute the questionnaire to dozens, hundreds and sometimes thousands of suppliers (mostly via e-mail). Subsequently, the organization must verify that each supplier has received the questionnaire, actually understands what is expected of it, and knows how to respond to the specific questionnaire from that particular organization. Finally, the organization must analyze all of the questionnaires and make decisions based on the replies sent to it. A data/cyber-security expert is needed, who must devote a considerable amount of valuable time to these operations.
- Organizations are not succeeding in keeping up with the volume of their supplier audits in terms of the number and scope of the audits.
- Suppliers, on the other hand, are forced to appoint experts and allocate considerable resources to handling the cyber defense requirements of their various customers: complete a variety of different questionnaires, comply with the various requirements received from each organization, respond to all organizations who contact them with regard to cyber defense issues, prepare for audits to be conducted on their premises by consultants from organizations contemplating agreements with them, etc.



Organizations are exposed to a variety of potential risks in managing their supply chains, either from suppliers and/or from subcontractors that are providing a product or service to the organization. Consequently, organizations must be aware of the risks and constantly manage them. Risk management includes mapping the risks, categorizing them (in terms of criticality), appointing the risk management officer and defining the controls that must be assimilated in order to mitigate the risk to the extent possible or, alternatively, to assume or transfer the risk.

If a supplier or sub-supplier providing a product or service to the organization has inadequate data security measures in place, this could jeopardize the company.

Below are some examples of potential risks (shortcomings) originating from supply chains that organizations must manage:

- Leaks of the organization's data due to improper storage on a cloud (e.g., as a result of misconfiguration).
- Information loss resulting from suppliers losing equipment, such as laptops or USB devices.
- Reputational damage resulting from corruption of the company's data stored on a cloud.
- Infringement of the privacy of the company's employees due to intrusion of a communications channel used by suppliers to transfer deliverables to customers.
- Undermining business targets as a result of the theft of patents or business plans saved on the company's servers.
- Data disruption arising from incorrect coding by a software supplier.
- Disabling business targets due to denial of service that paralyzes a supplier's computer resources (e.g., as a result of ransomware on a supplier's network).
- Leaked business information due to a supplier's negligent personnel management procedures relating to employee severance.
- Malware infecting the organization's network as a result of unsecured connections between the organization's network and a supplier's network.

- 4 This lack of standardization constitutes a market failure that should be corrected. The Israeli economy considers the National Cyber Directorate to be an objective, professional government body with a comprehensive perspective on the economy and consequently to be well-placed to act on behalf of the State in addressing this market failure. Furthermore, by virtue of its responsibility for the cyber defense of the government and the State of Israel's critical infrastructure, the Directorate has a duty to address this market failure by assisting the organizations under its guidance.

5 The meeting with suppliers, customers, regulatory authorities and consultants held throughout 2018 ascertained that two issues need to be promoted in order to help organizations in the economy optimally manage the process:

1. Uniform language: Standardizing requirements issued to suppliers may help organizations (suppliers and customers) save time developing a requirements document, supported by questions, etc. The current situation, with each organization developing its own questionnaire, is a burden for both customers and suppliers. Creating a uniform language in the economy will reduce the burden at the planning stage as well as at the control and audit stages.



2. Building a reliable mechanism of trust in the market: To save organizations time and money, both sides of the commitment (supplier and customer) must ensure that the mode of inspection and level of substantiation are being performed professionally. The current situation with many organizations conducting inspections/reviews of the same supplier is a burden for both supplier and customer. To address this, it is possible to work out the widest common denominator that is compatible with many organizations in the economy (e.g., maintaining logs, compliance with privacy protection regulations, backups, defense tools to protect terminal stations and the network, etc.). Although suppliers do sometimes “go through the process” for a particular customer, even through an independent consultant, they are often required to answer the entire questionnaire multiple times for other customers in the economy. Due to the difficulties that organizations face in auditing multiple suppliers, customers often “make do” with sending a questionnaire and relying on a “read and sign” approach.



Example: Let's say that organization A knew that a particular supplier has been asked questions regarding its cyber security controls that are important to it, and the supplier even proved those through a third-party certified auditor. Organization A might not be required to perform auditing of this same supplier. Since that supplier provided a broad common denominator of professional proof of his cyber defense measures that should satisfy a substantial segment of the economy. Even if organization A may want to inspect additional issues, it shall emphasize the efforts on it's residual risk only.

6 This is why the Directorate developed the National Methodology for Supply Chain Protection (hereinafter, “the Methodology”), which regulates the cyber defense activities of the supply chain in the Israeli economy. This Methodology addresses the level of services offered by the State and issues recommendations to organizations about processes for managing cyber risks from the supply chain and cyber defense recommendations to suppliers.



Cyber Israel

Prime Minister's Office
National Cyber Directorate

SCOPE

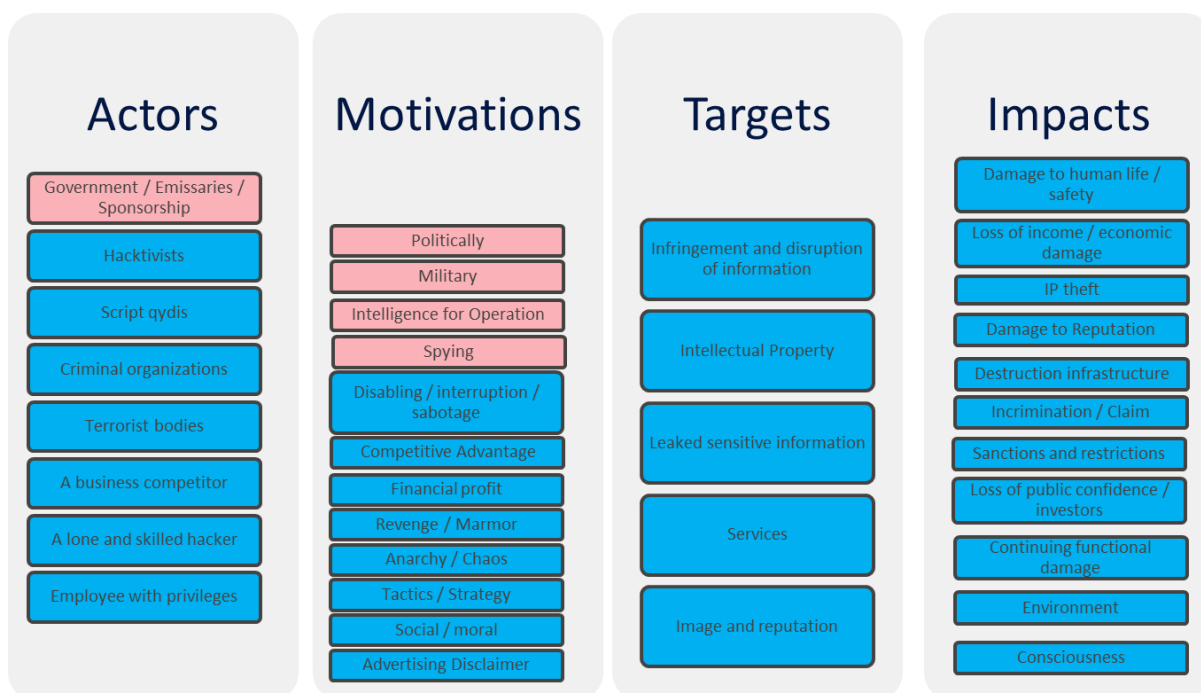
1





- 1 The purpose of the initiative is to increase suppliers' cyber defense capabilities against many types of cyber-attack. Although the initiative does not purport to prevent an attack by a strong and determined attacker, such as a State-level advanced persistent threat (APT), under the current situation many attackers do not need sophisticated tools to hack into an organization through a supply chain that lacks basic cyber security measures. The initiative will nevertheless raise the bar by enhancing the economy's cyber defense mechanisms against formidable attackers.

The Following Scheme Describes The Scope Coverage Of The Initiative
(Marked In Blue)



- 2 There are instances where additional or distinct activities are required. For example:
 - Some suppliers are incapable of complying with the cyber defense requirements expected of them, but organizations want to contract with them anyway for particular reasons such as an existing contractual obligation, the supplier's specific know-how and expertise, or for other reasons. In these instances, a risk management process needs to be implemented with regard to that specific supplier and risk-mitigation decisions must be made, for example, by implementing compensating controls, by developing a different work process with the supplier, etc.
 - There are suppliers with which the average customer has no leverage with regard to their level of cyber defense. Sometimes this derives from the "power ratios" between the supplier and the customer; sometimes the source of the problem is a foreign supplier and the customer is unable to conduct audits or require that it comply with specific cyber defense



requirements, etc. In these instances, customers can try to apply pressure on the supplier through other channels such as referral to the regulatory authorities, or several customers can organize a group to put pressure on that supplier. It is also sometimes possible (if there is no effective way to verify a supplier's level of cyber defense) to rely on existing international certification (such as SOC2) and include contractual provisions requiring audits or reception of information. Frequently, these suppliers grant their customers access to the results of risk surveys conducted through an independent third party. Reviewing risk surveys may provide customers with important details. In these cases, it is important to ascertain the scope of the audit, because certification may be issued for a particular service/product and not for the supplier's entire operations. Furthermore, it is critical to understand the division of responsibilities between the supplier and the customer in terms of cyber defense. For example: the fact that the provider of international cloud services is complying with the requirements of the customary standard in this field (such as CSA²), does not automatically attest to the division of responsibility³ with regard to the management of software updates, user management, firmware, backups, monitoring, etc. The use of an RACI matrix (Responsible, Accountable, Consulted, Informed) will help to better manage the risk.

- Suppliers which, if attacked, might cause severe damage to an organization's core operations. In these instances, in addition to performing a review to assess the organization's level of cyber defense according to this Methodology, it is also recommended to perform individual risk assessment surveys. This type of survey will take into account the designated information, specific business processes, mapping of specific threats and threat attribution, etc.

² <https://cloudsecurityalliance.org/>

³ See for example: <https://www.cloudsecurityalliance.no/2019/02/mapping-of-on-premises-security-controls-vs-major-cloud-providers-version-3-2-feb-2019/>



Cyber Israel

Prime Minister's Office
National Cyber Directorate

DELIVERABLES OF INITIATIVE





Improved Professionalism in Organizations: Use of the “Cyber Defense Methodology for Organizations” to manage cyber risks originating from the supply chain. This document helps organizations map suppliers, prioritize them according to the degree of risk that they pose for the organization, assess the specific risk that they pose to the organization and define cyber defense requirements from their suppliers (see appendix).



Supplier Questionnaire: Modular set of requirements for suppliers in the economy. These requirements are divided according to the degree of risk that the supplier poses to an organization’s business processes and its systems (material/immaterial supplier) and according to the nature of the agreement (supplier of a cloud-based service, supplier that is a software developer, supplier receiving remote access, etc.) (see appendix).



Supply Chain Module in the Organizational Goals and Controls System: The National Cyber Directorate has developed this supplier-management module as a free and accessible service to the economy. The module enables suppliers to complete the questionnaire online easily and intuitively and, after the supplier has recorded its replies to all of the questions, a detailed report is produced that contains graphic analyses to illustrate the supplier’s cyber defense situation and indicates the controls requiring improvement and those needed to streamline the construction of a work plan (see appendix).



Certification of Qualified Supply Chain Inspectors: State accreditation of experts who have met the threshold criteria (including threshold data, an entrance examination and an admissions committee), and who have completed specialized training in the inspection of cyber defense capabilities in organizational supply chains according to the Directorate’s methodology and successfully passed the certification exam. The certificate is issued by an authorized certification body on behalf of the National Cyber Directorate, and the suppliers are registered in the national database (see appendix).



Telephone Support Center “119”: Platform providing support and assistance on topics relating to a supply chain, including answers to methodological questions and to technical questions about the Supply Chain Module and the Directorate’s website.



Supplier Certification: State regulation of the certification process for approved suppliers. The supplier certification process is performed by a certification body on behalf of the Directorate and includes inspections by a certified supply chain inspector, approval by the certification body, the issue of certificates to suppliers and registration of certified suppliers in the national database (see appendix).



National database: National database that will be accessible on the Directorate’s website, which includes a list of certified supply chain inspectors and a database query function to identify certified suppliers (see appendix).

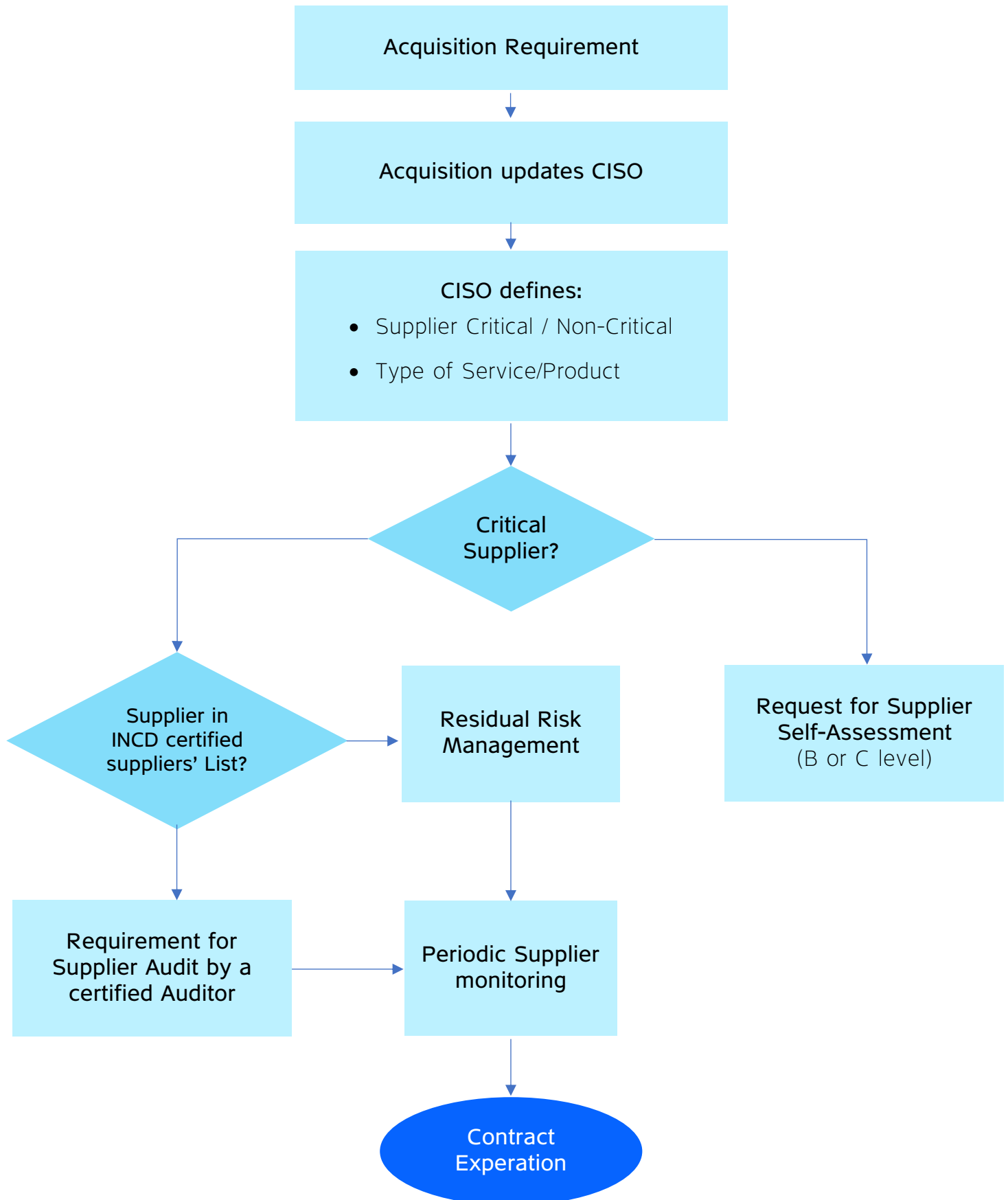


Cyber Israel

Prime Minister's Office
National Cyber Directorate

Description of the Process
from the
**ORGANIZATION'S
PERSPECTIVE**







The organization must map the risks originating from its supply chain and must perform operations in two key channels in order to protect itself from cyber-attacks through its supply chain:

- a. Operations performed by the organization itself: These operations include measures such as mapping and classifying suppliers, obtaining suppliers' signatures on declarations and relevant contracts, incorporating provisions relating to cyber defense in their contracts, performing controls and audits, acquiring and implementing monitoring tools, formulating and implementing a remote connection policy, content disarming and reconstruction (CDR) in relation to content being uploaded to the organization's network, hostile media blocking, authorizations management, compartmentalization, etc.
- b. Operations that the organization requires of its various suppliers for implementation by the suppliers themselves and/or on the suppliers' premises before contracting with them. These operations include requiring the supplier to develop software in a particular configuration and harden its communications equipment, devices, servers and terminal stations, requiring the supplier to protect the service that it is providing through technologies for the prevention of denial-of-service attacks, requiring backups, etc.

To this end, the organization should:

- Map its suppliers according to:
 - Structural categories (deriving from the nature of the risk) - general services, provision of remote access, cloud services, software development;
 - The materiality/immateriality of the supplier according to the potential losses that might be caused to the organization as a result of a cyber-attack on the supplier (ranking structured for the Israeli economy);
 - The required level of proof: statement, attestation supported by evidence, or control by an independent certification body;
- Refer its suppliers to the Directorate's website for the purpose of completing a Supplier Questionnaire, based on the nature of the risk, the potential harm from the supplier and the required level of proof;
- Analyze the questionnaire, the required supporting documents and/or the required certification (according to that stated above) and ascertain the level of residual risk from the supplier;
- Incorporate supplier risk management in the organization's cyber risk management system;
- Incorporate the necessary controls in the contracting process: purchasing aspects, organizational policy, supplier contracts and supplier briefing;



Cyber Israel

Prime Minister's Office
National Cyber Directorate

- Incorporate the necessary controls over the term of contract to protect sensitive operational data (and particularly OT data) and add compensating controls;
- Incorporate the necessary controls upon concluding the agreement.

For details, see the appendix.



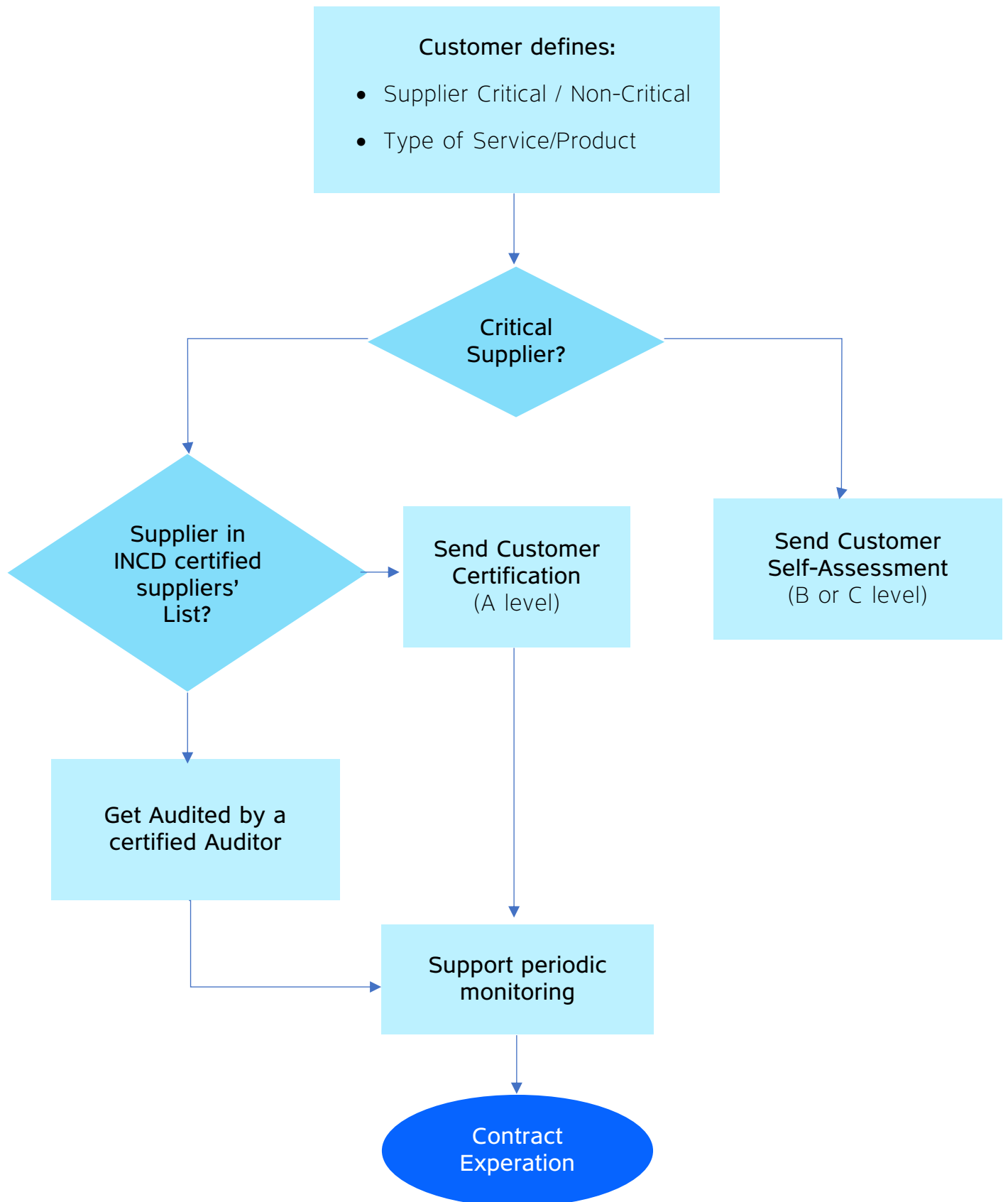


Cyber Israel

Prime Minister's Office
National Cyber Directorate

Description of the Process
from the
**SUPPLIER'S
PERSPECTIVE**







Cyber Israel

Prime Minister's Office
National Cyber Directorate

- 1 The supplier will complete the questionnaire on the Directorate's website about the state of its cyber defense measures, based on the services it provides to its customers, including the actual versus the desired situation (given anonymously).
- 2 Suppliers ranked at level C must forward the questionnaire to the organization after having it signed by an authorized signatory.
- 3 Suppliers ranked at level B must forward the questionnaire to the organization after having it signed by an authorized signatory and accompanied by supporting documents as defined in this Methodology (for the purpose of ascertaining the effectiveness of the requisite cyber defense controls).
- 4 Suppliers ranked at level A must complete the questionnaire in conjunction with a supply chain inspector who has been certified by the Directorate and must forward the questionnaire signed by an authorized signatory, accompanied by supporting documents as defined in this Methodology, to the certification body in order to obtain an official certificate. The certificate and, if necessary, all other material, will be forwarded to the organization. Certification will have to be renewed periodically, as defined in this Methodology.

For details, see the appendix.





Cyber Israel

Prime Minister's Office
National Cyber Directorate

Description of the
**REGULATION
PROCESS**



1 **The regulation process will regulate the following services**

The Cyber Directorate's regulation process includes the Cyber Directorate as the sole accreditation body, certification bodies such as the Israel Standards Institute, inspection bodies that inspect the supply chain and the customers in this process - the certified suppliers.



- **Regulation by certification bodies on behalf of the Cyber Directorate**

A pilot process has been defined with the Israel Standards Institute as the first certification body:

- Supply chain inspectors operating on behalf of the Directorate.
- Suppliers certified by the Directorate.

This process defines the interfaces between the National Cyber Directorate and the certification body, and between them and the inspection bodies and suppliers. The certification body is also required to provide training services for the purpose of qualifying supply chain inspectors according to the Directorate's methodology.

A public appeal to the economy for the establishment of additional certification bodies is underway.

- **Regulating supply chain inspectors (certified Auditors)**

Admissions criteria to a certification course for supply chain inspectors have been defined. These inspectors are certified on behalf of the Directorate for the purpose of assessing the quality of the answers in the Supplier Questionnaires and the evidence required in order for a certificate to be issued by the certification body. The admissions criteria are very stringent (including considerable relevant experience in performing cyber defense audits, a professional entrance examination in cyber defense and a personal interview), and are intended to screen for high-caliber inspectors, in consideration of the fact that maintaining the economy's confidence depends on high-quality, independent professional inspectors. The short course provides instruction in the Cyber Directorate's Methodology and in the supplier certification process.

- **Regulating certified suppliers**

The supplier certification process has been defined, from the submission of an application for certification and until the issue of a certificate, the validity of the certificate, etc. The goal of this process is to minimize the burden on suppliers, while maintaining the high quality of the process and its outcomes, in order to ensure that the certification is reliable.

For details, see the appendix.



Cyber Israel

Prime Minister's Office
National Cyber Directorate

Appendix A

THE PROCESS

from the Organization's Perspective



Process of protecting against cyber risks from the supply chain from the perspective of an organization in the Israeli economy (particularly from the perspective of the organization's cyber defense officer and data security officer).

This is an orderly and practical methodology for managing cyber defense of the supply chain, accompanied by a set of detailed controls that are recommended for implementation by all organizations in the Israeli economy for the purpose of ongoing effective management of the supply chain.



Supply chain management encompasses the cycle of the organization's activities with regard to service providers and product providers, which begins at the preliminary stage of mapping and classifying the organization's information assets, followed by mapping of the suppliers with whom the organization will contract. Suppliers must be inspected periodically over time, using a set of predefined criteria and measurements. During its agreements with suppliers, organizations must constantly perform risk assessments and take action accordingly.

It is important to emphasize the necessity of incorporating in comprehensive agreements with suppliers all of the criteria and service levels required in order to meet requisite standards of data security for each service/product. Organizations should institute orderly procedures and document the supplier selection process and the procedures for managing their agreements with suppliers. Furthermore, organizations should provide comprehensive training about data security aspects to all supplier employees who are expected to be involved in the agreement with the organization. Another critical issue is the process of terminating an agreement with a supplier. Organizations must ensure the correct execution of all provisions in their supplier agreements relating to the deletion of the organization's data and the cancellation of the supplier's access authorizations.

The set of controls and the emphases presented hereunder represent an orderly methodology for managing an organization's supply chain.

Organizations' cyber defense activities against supply chain risks can be broken down into the following stages:

Operations vis-à-vis suppliers



1 Supplier mapping

- A list of the organization's suppliers should be prepared, including various types of service providers such as: software development, hardware and communications providers, companies implementing and assimilating systems in the organization, consulting and risk survey firms, and service providers such as accountants, lawyers, printers, copy editors, branding, technical support, integration, etc.
- The list should be validated by business professionals in the organization who are familiar with the activities with the aforementioned suppliers. It is recommended to involve purchasing personnel in this process and in preparing the list, as well as personnel from the IT systems department (in order to identify external software, IT service providers, suppliers with remote access to the organization, etc.).
- An organizational process should be instituted to ensure that the cyber defense personnel will be aware when any new supplier is added and when any new agreement has been signed. For example, this can be implemented as part of a working procedure in the organization and as part of involving the data security/cyber defense department in the process of opening a new supplier account in the financial department and in the information system, etc.
- Supplier mapping should include references to the type of service being provided by the supplier, including references to the following categories:
 - **Remote access:** Suppliers that need to connect to the organization's resources as part of the agreement with them in order to provide the product/service. In such instances, the supplier is expected to work in compliance with the organization's security policy regarding remote connectivity. However, there are situations when the supplier defines its mode of remote connection to its customers. In these cases, the organization must verify that the mode of connection is being performed safely. In many instances, these suppliers are computer/IT/communications/development firms that could potentially cause major damage to the organization. For these services, specific controls and defense requirements are specified in the Supplier Questionnaire.



- **Cloud services:** Suppliers who provide SaaS or PaaS within the scope of the agreement contract. These suppliers include the customary cloud services, such as SaaS, PaaS and IaaS. These types of suppliers include for example: site storage companies, information systems having access to the organization via a cloud, online services that the organization uses, etc. They can also include suppliers whose availability is critical for the organization and those for which the degree of confidentiality and information reliability are particularly sensitive. For these services, specific controls and defense requirements are specified in the Supplier Questionnaire. Please note: this category is not intended for cases in which information is stored offline (such as storage of backup tapes, documents, etc.).
 - **Software development:** Suppliers that develop software that is installed in the organization. These suppliers may represent a potential security breach. The level of the organization's cyber defense depends largely on the level of cyber defense in the development processes and life cycle management of the supplier developing the software. For these services, specific controls and defense requirements are specified in the Supplier Questionnaire.
 - **General requirements:** Every supplier is required to maintain a basic level of cyber defense in relation to various issues, regardless of the type of service that it provides. These requirements represent the minimum required from every supplier with whom the organization contracts, according to the level of risk deriving from the agreement with it (material/ immaterial supplier). Suppliers in this category can include for example: branding companies, survey firms, various types of consulting firms (cyber advice, operational advice, strategic advice, etc.), lawyers, accountants, companies providing translation services, printers and other suppliers if a cyber-attack against them will jeopardize their customers due to information exposure and other risks.
- At the end of this stage, organizations will obtain a mapping table that contains at least the following aspects:

Supplier Mapping				
Supplier's name	Type of service/product that it provides	Organization's business contact with the supplier	Contact details of supplier's representative in charge of cyber defense	Type of services being provided (cloud-based, software development, remote access, general requirements)

2 Ranking of suppliers:

- Suppliers should be ranking according to three risk levels. These levels are presented in the table below (with relevant values and columns).
- Supplier ranking should take into account the repercussions / potential damage that is liable to be caused to the organization as a result of a cyber incident in a supplier's system. A number of criteria may be used to calculate the potential damage, such as those presented in the table below:

Supplier rank	Level of expected damage to the organization from the supplier	Economic damage to the organization (including costs resulting from loss of revenue, reputation, regulations etc.)	Damage to business continuity	Sensitivity of the data accessible by the supplier	Probability of the occurrence of a cyber incident resulting from an agreement
C	low	Tens of thousands of shekels	Recovery from a cyber incident at a supplier's will take several hours	Information is not very sensitive	Low dependence on cyber. Examples: supplier of office equipment, expert services not involving the organization's information, and no access authorizations to the organization's systems, etc.
B	Moderate	Hundreds of thousands of shekels	Recovery from a cyber incident at a supplier's will take several days	Information is moderately sensitive	Moderate dependency on cyber during the agreement with the supplier
A	High	More than 1 million shekels	Recovery from a cyber incident at a supplier's will take several weeks	Sensitive business information, such as patents, trade secrets, etc.	High dependency on cyber, such as: IT service providers, with remote access authorizations; software equipment suppliers; suppliers holding sensitive material in a cloud or in systems on the supplier's premises

Request from the Government Advertising Agency: Add a sample decision-making hierarchy diagram to illustrate the table and add the word "sample" as a watermark behind the table.

- Working with the above table will help rank suppliers according to the various criteria. A supplier's final ranking (out of the three levels: A, B or C) will be based on the maximum potential damage. For example: a supplier that is ranked at level A in one criterion will be ranked as a supplier with a potential damage level A even if it is ranked at level C for the rest of the criteria.
 - Suppliers ranked at level A will be required to prove their level of cyber defense in the requirements in the Supplier Questionnaire through a certified supply chain inspector. For the list of certified inspectors, see list on the Directorate's website and in the regulation module.



- Suppliers ranked at level B will be required to complete the Supplier Questionnaire and attach evidence as required in the questionnaire. The supplier will forward the evidence to the customer through a secure channel to be agreed upon between the parties.
- Suppliers ranked at level C will complete the Supplier Questionnaire and will obtain the signature of an attorney or the company's CEO on a supplier's statement regarding the level of compliance with the cyber defense requirements in the questionnaire.
- At the end of this stage, organizations will have obtained a map of the suppliers with the ranking of their risk level and the degree of criticality of each of them.

Supplier Mapping					Supplier rank
Supplier name	Agreement characteristics	Organization's business contact with the supplier	Contact details of supplier's representative for cyber defense-related questions	Category of service being provided (cloud-based, software development, remote access, service involving exposure of customer information)	Supplier's level of risk (material or immaterial supplier)
DEMO A strategic consulting	Assisting the organization's management in building a strategic plan	Anat	XYZ	General requirements - drafting of sensitive documents for the organization. The supplier holds sensitive management plans regarding new spheres of business that the organization plans to enter in the coming years	Yes
DEMO B ERP implementer	Implementing the system opposite the operations department	Israel	ABC	Software development - assists the IT systems department with implementation of the system	No
DEMO C website development and storage	Storing the company's website (including upgrades, maintenance, etc.)	Or	AAA	Cloud storage and maintenance of the company's website	Yes
DEMO D integration	Support of equipment and communications	Eli	BBB	General requirements - supplier has no remote access and its work focuses on assisting the company's communications personnel	No
DEMO E law firm	Patent drafting	Israel	CCC	General requirements - the supplier holds sensitive information about the company in his personal computer and on USB devices	Yes

3 Assessing the supplier's level of cyber defense:

- For the purposes of assessing a supplier's level of cyber defense, organizations should require their suppliers to comply with the cyber defense requirements pursuant to this Methodology. To this end, organizations will define the following supplier parameters:
 - Does the organization consider the supplier to be material to it⁴? For the purpose of tailoring the cyber defense to the risk arising from contracting with the specific supplier, organizations must define whether or not a supplier is material. This determination affects the amount and extent of the controls required of it. For example, a supplier that is not defined as material will be required to maintain basic backups, while a supplier that is defined as material, will be required to maintain and implement more advanced controls. Note: some standards and regulations contain definitions of "material supplier."
 - Relevant category of service: Organizations should inform their suppliers about what is expected from them within the scope of the agreement in terms of remote access, software development, etc. Although there are minimum general requirements in every agreement, in instances when the agreement includes special duties, such as development processes, the supplier is required to comply with additional cyber defense aspects that are specified in the Supplier Questionnaire in this Methodology.
 - Expected response: organizations must inform their suppliers whether they must complete the report using a self-declaration form that they produce from the system, whether they must attach supporting documents according to the requirements of the questionnaire, or whether they must prove compliance with the Methodology's requirements through an independent party (such as a certified inspector).
- If a supplier is already certified, an organization might be satisfied with receiving the survey results or adding a few specific requirements.
- It is recommended that an annual work plan should be drawn up defining the schedule for sending cyber defense requirements and to which supplier, including a template for a standard cyber defense requirements letter, which will streamline the process in the organization and verify that all relevant suppliers have been contacted (according to the organization's risk management plan).



Note: the level of risk of some suppliers may be affected by regulatory aspects or the supplier may be listed as a supplier in times of national emergency.

⁴ Material/critical supplier: Supplier who provides services such as: information systems support and/or maintenance, storing of sensitive information off the organization's premises, technological outsourcing services, etc. (Proper Banking Practices 363 - Managing Cyber Risks in the Supply Chain, clause 7), or a supplier when damage to it is liable to cause material damage to the organization. The decision on defining a supplier as material is at the organization's discretion. An exception to this is when a regulatory authority has defined in advance for organizations in the economy over which it is responsible that a particular supplier, or any supplier that meets defined criteria, constitutes a material supplier in any event.

4 Managing the residual cyber risk

From a supplier Decision-making with regard to managing the risks when contracting with suppliers: in some instances, despite the need to contract with suppliers maintaining an adequate level of cyber defense, an organization's management may be required to sign an agreement under any circumstances. In order to manage risks effectively, it is recommended to keep in mind the four alternatives in risk management:

- Accepting the risk: In this instance, the potential risk must be presented to the organization's management, and the fact that a decision was reached to not take special measures during the agreement with that supplier. This can be instances in which the supplier is immaterial, in which case, the organization decides not to send cyber defense requirements to it, or instances of major dependence on a supplier that is not prepared to comply with the cyber defense requirements, but the organization contracts with it anyway due to other constraints and for other reasons.
- Transferring the risk, for example, by purchasing insurance to cover losses of this type.
- Mitigating the risk, such as by adding compensating controls opposite the supplier.
- Rejecting the risk, such as when the management recommends not renewing the agreement or immediately terminating the agreement with the supplier.



Intra-Organizational Operations



Risk map

After completing the procedures for the organization's existing agreements with suppliers - mapping, ranking, assessing suppliers' level of cyber defense and managing suppliers' residual risk, as described in this document - a risk map should be drawn up, which should be maintained and regularly updated by the organization's cyber defense officer and periodically approved by the organization's management.



Purchasing aspects

Organizations' agreement process should take into account the cyber defense aspects presented in this document in a structured process.

- When contracting with a new supplier, the cyber defense officer should be informed automatically. If possible, the supplier management system should automate this process and add fields to characterize the supplier's cyber defense details (such as: contact person, supplier ranking, the services that it provides, etc.). If possible, the process of setting up a new supplier in the system should be made contingent upon approval by the organization's cyber defense/data security officer.

- When renewing an agreement with an existing supplier, organizations should make sure that the contract renewal takes into account the supplier's current level of cyber defense and the procedures for meeting the recommendations to remedy shortcomings that the organization found at the supplier's.
- Periodically, a comparison should be made between an organization's suppliers and the list of certified suppliers in the Certification Module of the organizational goals and controls system.
- The organization's management should allocate the resources needed to perform audits of material suppliers according to their definition by the relevant business officer in the organization and the potential losses they could cause.



Policy for assessing risks in the supply chain

- A work procedure should be drafted, approved by the management and validated periodically.
- An organization's policy should include reference to compensating controls in those agreements in which it is not possible to bring the supplier to the required level of cyber defense. These controls may include, for example, the establishment of a supplier environment in the organization, providing hardened computers and equipment to suppliers, deciding that particular types of work by a supplier will only be performed on the organization's premises, etc.
- The organization's policy should include reference to management tools for controlling the process. These tools may be helpful to the organization both during the supplier mapping and assessment stage and during the follow-up stage to ensure that the recommendations and tasks with regard to the various suppliers are being implemented. These are familiar tools in the economy, such as GRC (governance, risk management and compliance), or VRM (vendor risk management). The advantage of using these tools lies in the ability to obtain a holistic picture of the status of the suppliers, as well as alerts, presentation of a benchmark situation report, automation of communications with them and of the assessment of the supplier's level of cyber defense, etc.
- The organization's policy should also include reference to the following aspects: changes in the type of agreement with a supplier and in the supplier's organizational/technological structure, aspects of control and auditing, suppliers' mode of remote access, aspects of uploading information to a cloud, handling of data security incidents at a supplier's, procedures for terminating agreements with suppliers, and the frequency and mode of cyber defense queries to the various suppliers according to the requirements of this Methodology.
- The organization's policy should define the party responsible for protecting information held by a supplier (throughout the entire chain of custody, including suppliers and suppliers' third parties).



The agreement: An agreement should be signed with the supplier containing all aspects of managing cyber risks in the supply chain. A sample agreement is attached in Appendix. Incorporating cyber defense aspects in contracts and agreements should be anchored in a work procedure that has been coordinated with the organization's purchasing department. Particular attention should be paid to existing long-term contracts. In these cases, it is often more difficult to convince the supplier to enhance its level of cyber defense. It is recommended that the organization's purchasing department should analyze ways to motivate suppliers to meet the cyber defense requirements expected of them.



Supplier briefings

- Before a supplier begins working or becomes exposed to the organization's system, either physically or electronically, each of the supplier's employees who participates in the agreement should be briefed on the following subjects:
 - The relevant threats to the system;
 - The potential losses resulting from a cyber attack on the system;
 - Details of directives that they will be required to comply with and implement.
- The briefing should be presented by a competent professional in the organization who is an expert in the cyber defense requirements that must be met in order to minimize the organization's exposure to risks to the extent possible.
- After the briefing, all of the supplier's employees should sign a declaration in which they undertake to implement the security requirements.
- The declaration documents should be kept by the organization for a minimum of two years or as needed after the agreement with the supplier has ended.



Controls to be implemented during the term of the agreement

- If a supplier works on the organization's premises, the organization should ensure that the activities are being carried out according to the same directives as imposed on the organization's employees.
- If a supplier works from its own premises, the organization should send a cyber security requirements document to the supplier before it begins working or is exposed to the organization's system, whether physically or electronically.
 - For material suppliers, the organization should perform audits at least annually at the supplier's premises in order to verify that the supplier is implementing the cyber security directives.
 - For material suppliers, it is recommended to consider using monitoring tools capable of providing real-time indications and continuous monitoring of the supplier's level of defense (continuous control monitoring).
- The organization should define those activities in relation to which the supplier is required to use strong means of identification.

- The organization should be prepared to operate during a data-security incident, contractually, technologically and through processes.



- Due to the risks incurred due to a supplier's remotely accessing the organization's systems during its activities (if relevant), it is essential for organizations to maintain security and control mechanisms to help minimize these risks, such as:
 - Using a separate designated environment with a virtual configuration.
 - Internet connections to the organization's systems should be done using a session protocol that differs from that used when connecting the separate environment to the organization's systems.
 - Accessing this environment should be in a white list format and should limit the workstations and addresses having authorized access, the protocols, the connection times, the duration of an active connection, and disconnection in case of inactivity, and limit applications with authorized access.
 - The environment should be returned to a secure steady state at the end of use.
 - The duration of an active connection should be limited and disconnected if inactivity is detected.
 - The user account for access from outside should be different from that used for internal access and should have different identification and authentication data.
 - Authentication should be based on two different factors out of the following alternatives: a designated OTP component that is not connected to media, a smart card, biometrics or a password.
 - The account and authorizations at the level of application for remote access should differ from those used for internal access.
 - Users should be prevented from being simultaneously connected to networks or systems locally and remotely. An alert should be built in for any such instance.
 - All applications at a workstation should be operated using a white list format and prevent any opening of unauthorized applications.



- The identification and authentication data for a remote management account should differ from internal management accounts and be managed in a designated group.
- The organization should define that any user with remote access will only receive the access authorizations necessary to perform management operations that are permitted via remote access, as defined by the competent professional on behalf of the organization.
- Traffic recording and monitoring should be performed for the entire duration of the connection, anomalies and deviations from authorized management operations should be identified as well as deviations from the cyber security policy (suppliers should be informed that all of their operations in the organization's systems will be recorded).
- Suppliers should be prevented from gaining unauthorized access to the organization's systems, particularly the production environment.
- The organization should ensure secure access and isolate its operations from all of its suppliers' work environments.
- The organization should draft a written procedure outlining the supplier connection process for the purposes of managing or maintaining system components on the network, while referring to the following:
 - Connection and approval of operations: solely by the competent professional on behalf of the organization.
 - Mode of monitoring and recording
 - Receiving alerts and handling anomalies.
 - Discontinuing operations and closing connections.
 - Verifying disconnections from the organization's systems.
- An ability to immediately disconnect a link should be created in the event that an anomalous incident is detected.
- The possibility of adding and/or removing files in this channel should be prevented, which will only be enabled in a separate channel for content disarming and reconstruction (CDR), DLP, media blackening.
- Due to the risks incurred when an external supplier has access to the organization's facilities (if relevant), it is essential for organizations to maintain security and control mechanisms to help minimize these risks, such as:
 - For activities by a permanent supplier, a designated organization computer should be provided containing all applications needed for the supplier's activities.
 - For ad hoc activities, such as penetration tests, vulnerability reviews, etc., the volume of the supplier's activities should be clearly and precisely predefined, along with indicators of success and failure, incidents and responses in the event of a malfunction, and an internal staff member should be appointed to actively supervise the supplier's employees.
 - Existing management passwords should not be disclosed to suppliers. If necessary, a temporary designated account should be opened with authorizations that are needed solely for that particular activity.

- If management passwords are disclosed for the purpose of an activity, they should be changed immediately thereafter.
- Relevant personnel should be informed about the beginning and end of the activity, in order to increase their alertness and the sensitivity threshold for anomalous incidents.
- Any activity being performed by a supplier in the organization's systems (such as penetration tests, vulnerability reviews) should be carried out while minimally compromising the cyber security level and after analyzing the implications of the risks arising from such activities.
- At the end of the activity, a test should be performed to ascertain what operations were actually performed and the temporary accounts and authorizations allocated for the activity should be closed.



Protection of sensitive operational data

- Sensitive operational data are data that relate to the operation, maintenance, security measures and management of the systems, when, in the event that they are attacked, they are liable to enable shortcuts to be taken during an attack on critical systems and/or theft of sensitive information, such as:
 - User names and passwords;
 - Network topology (such as network diagrams including IP addresses);
 - Parameters of data security equipment and communications (such as FW rules and communications definitions);
 - Technical/operational data about the system (such as operating manuals, source code);
 - Photographs of particularly sensitive areas and components (such as server rooms and communications equipment);
 - Backups containing data files and databases;
 - Information about the temporary reduction of the data security measures in the system for the purpose of performing maintenance and updating operations.
- Sensitive information should be securely stored, including encryption and restricting access to solely authorized personnel.
- Monitoring should be performed to detect any attempts at accessing and using information, including unsuccessful attempts.
- Unauthorized personnel should be blocked from sending classified information outside the organizational network using designated means for this (such as DLP). Verify that the identification of sensitive/privileged information also includes reference to sensitive operational information.
- Classified operational information should be forwarded to an external party solely via a secure configuration (encrypted e-mail) or a secure file transfer mechanism (such as safes).
- The hard disk and the bios of laptops containing such information should be encrypted.



Protection of information in the industrial control systems (operational technology - OT)

- Most of the industrial control systems were designed a long time ago, before there was awareness of cyber threats. Therefore, these systems lack data security controls. Due to the increase in the internal and external threats targeting industrial and critical infrastructure, controls are needed that provide real-time detection and defense, while complying with the unique technical and operational requirements of the industrial control systems. For specific controls relating to industrial control systems, see the document on the National Cyber Directorate's website on this topic and/or the relevant documents published by leading standards organizations in the field.



Compensating controls and sanctions

- Sometimes, compensating controls are needed during an agreement with a supplier, in instances in which the organization cannot rely on the supplier's level of data security. The following are examples of compensating controls that may be implemented during an agreement:
 - The organization should provide a hardened laptop or hardened and designated workstation for the supplier's activities.
 - To the extent possible, the organization should require the supplier to perform its work on-site at the organization.
 - If the supplier does not work in separate environments, the organization should provide a safe environment through which the supplier will provide its services.⁵
 - The organization should test the supplier's system/service using internal tools and perform penetration tests before transferring the system/service to the production stage.⁶
- Sometimes it is necessary to impose sanctions on a supplier's activities. The following are examples of sanctions:
 - If a supplier fails to meet the criteria defined by the organization as critical for the purpose of the agreement. Agreements should be made contingent upon the performance of a supplier review during which the organization (or other party on its behalf) will perform an assessment of the nature and conduct of the supplier, before signing the agreement.⁷
 - If a supplier deviates from the organization's cyber-security directives, judgment should be exercised and, if necessary, the agreement should be terminated.
 - If a suspicion arises during the term of an agreement that a material supplier is exposing the organization to serious cyber risks, the organization should consider terminating the agreement immediately.

⁵ Control 16.4 of the Cyber Defense Methodology for Organizations.

⁶ Control 16.5 of the Cyber Defense Methodology for Organizations.

⁷ Control 16.3 of the Cyber Defense Methodology for Organizations.



Concluding an agreement with a supplier

- The organization should verify that arrangements with the supplier that were defined in the agreement are being carried out. It is particularly important to ensure that the supplier complies with all provisions relating to deletions of the organization's data stored at the supplier's site at the conclusion of the agreement between the parties. Inter alia, the following should be verified:
 - Verify that all records, media, equipment and components that belong to the organization and were used for the purposes of the supplier's work have been returned, including items held by all of the supplier's employees and subcontractors.
 - Additionally, the supplier should sign a declaration undertaking to not retain in its possession any components relating to a system and/or information about the organization, and that it shall not make any use of information about the organization to which it was exposed during the agreement.
 - Verify that magnetic media from any equipment used by the supplier during its agreement with the organization has been destroyed (e.g., if the supplier's computers were used to process and/or store information about the organization). Furthermore, the organization should verify the deletion of copies of files and information about the organization from the supplier's information systems and IT equipment once there is no longer any business need for retaining it.
 - The organization should verify that the supplier no longer has access authorizations, means of identification or physical and/or electronic access to the organization's information.
 - The organization should ensure that a directive has been issued about what is permitted and what is prohibited in relation to publicizing details of the project/agreement to third parties.





Cyber Israel

Prime Minister's Office
National Cyber Directorate

Appendix B

SUPPLIER QUESTIONNAIRE





The Supplier Questionnaire constitutes the fundamental elements required from suppliers in relation to agreements. This questionnaire is the minimum professional threshold, depending upon the type of agreement (such as: storage of information on a cloud, development, remote access, etc.), and depending upon the degree of sensitivity of the agreement (material or immaterial supplier). The questionnaire addresses risk management, creates transparency and uniformity in the economy with regard to cyber defense controls, and instills confidence about the organization's cyber defense response, its level of controls and its level of protection.

This questionnaire includes various cyber defense requirements according to the following structure:

Risk		Transparency and uniformity in the economy					Confidence				
Type of agreement	Materiality	Topic code	Topic	Control code	Control	Emphasis on implementation	Extent of implementation of the control	Required evidence	Emphases on testing	Threshold	Compatibility with standards

A link to the latest version of the questionnaire can be found on the Cyber Directorate's website (in Hebrew):

<https://www.gov.il/he/Departments/news/querysupply>

- Type of agreement: The various types of agreements, such as cloud-based services, software development, etc.
- Materiality: Defining whether the specific cyber defense requirement is expected from every supplier or only from material suppliers. The answer to this question is yes/no, whereby "yes" means that the requirement is expected to be implemented only by material suppliers.
- Topic code: Number assigned to the various requirement topics.
- Topic: Description of the general topic and its cyber defense requirements (such as: perimeter protection, backups and restorations, protection of terminal workstations, etc.).
- Control code: Code number assigned to the various control requirements.
- Control: Description of the specific requirement that the supplier is expected to implement.



- **Emphasis on implementing control:** General emphasis that helps to coordinate expectations between the supplier and the organization, and to explain through examples and additional emphasis, what the expectations are when referring to the level of cyber defense.
- **Extent of implementation of a control:** Details about the various ways to implement the control, with the answer ranging between “is not implemented” to “fully and effectively implemented” (and everything in between). The purpose of this column is to coordinate expectations with regard to the extent of the actual implementation of the control/requirement by the supplier. For example: the supplier is not expected to answer the question “do you have logs”/“do you perform backups” with a yes or no, but rather, the supplier is given the opportunity to explain to what extent the control is being implemented in relation to the organization.
- **Required evidence:** An explanation of the how the organization is to prove that the defined requirements are actually being implemented. Such evidence should be forwarded to the organization according to what was agreed upon between the parties.
- **Emphasis on external inspection:** Emphasis provided to an inspection body that will verify compliance before issuing a “rating” for the degree of assimilation of the cyber defense control requirements. This column is compulsory for inspections by certified inspectors.
- **Threshold:** Definition of the minimum degree of assimilation required for each control, while differentiating between a material supplier and an immaterial supplier. For example: on the topic of backups, the minimum extent of the control required from an immaterial supplier might be “1”, while for a material supplier, the minimum required might be “3.” Any supplier that fails to meet the threshold extent of implementation of the control is not meeting the organization’s expectations in relation to that specific topic.
- **Compatibility with standards:** Standards and regulations that apply to the supplier.



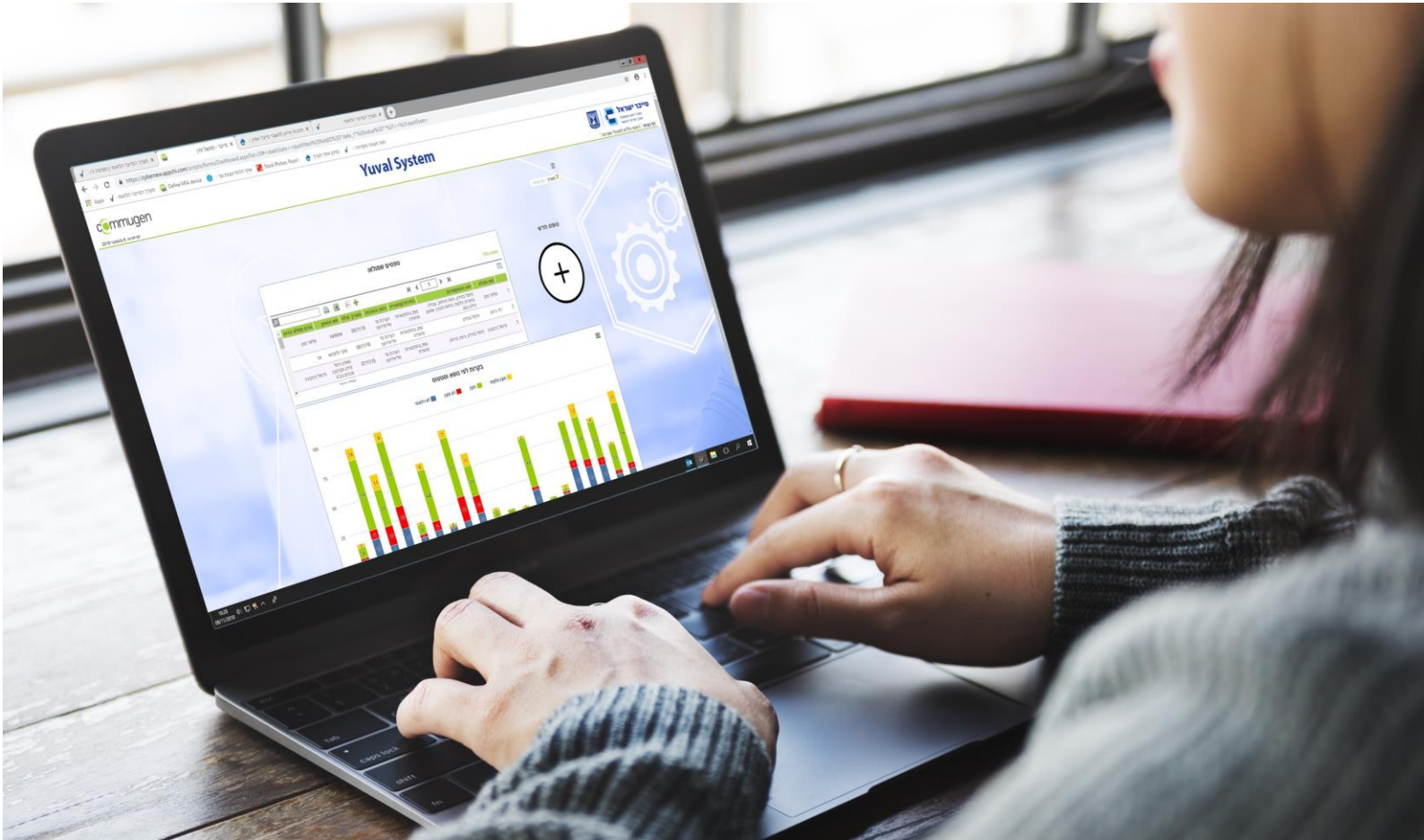
Cyber Israel

Prime Minister's Office
National Cyber Directorate

Appendix C

SUPPLY CHAIN MODULE





- 1 **Organizational goals and controls system is a national platform comprised of several modules. One of the system's modules is a Supply Chain Module that was developed for the purpose of providing a response to several challenges relating to managing the cyber risks in the supply chain that arose during the initiative. Some of the challenges found include:**
 - Scarcity of resources to support the stage of disseminating the questionnaire to a multitude of suppliers: Today, organizations are required to send their questionnaires to every single supplier, largely via e-mail. This process requires organizations: to maintain an updated list of the contact personnel at their various suppliers; to verify receipt of the questionnaire/the cyber defense requirements by their suppliers; to manage versions of the questionnaire and update suppliers if the questionnaire has been revised, etc. Once the questionnaire is digitized, every organization will be able to refer their suppliers to the system and be confident that their suppliers will find the latest version of the relevant questionnaire.
 - Scarcity of resources to add support personnel who will answer suppliers' questions about how to respond to the questionnaire: By using the system, suppliers will be able to obtain full answers to their questions about the cyber defense requirements, associated documents and tools - all centralized on a single platform.
 - A lack of uniformity in the structure of the deliverables of the review process: For the purpose of providing support to the control and auditing processes of the inspectors and certification bodies, the system guides the person completing the questionnaire through a structured process until a final report is produced at the end of the process. This report may constitute a self-declaration form if the process is carried out without a



certified inspector, and it can constitute the foundation that the inspector brings with him to the certification body if a supplier wants to apply for certification.

- Suppliers' difficulties managing the findings that arise during the review: Working with various applications and correspondence impedes the process of remedying shortcomings and issuing the updated situation to customers. The system enables suppliers to obtain their situation report in the form of easily-exported graphs and allows them to drill down in a particular topic, update the current level of defense and produce an updated report accordingly.
- Maintaining the principle of irrefutability: Today, the process of responding to cyber defense requirements is often carried out using various applications, such as e-mail correspondence, Excel, etc. Working with a structured system helps the recipient of the report know who responded to the report and when the report was produced, and to feel confident that the report was submitted in a format that is not an open file (such as Excel, since it is not easy to ascertain whether values were altered, when, by whom, what the original value was, where the latest version is, etc.).

The Supply Chain Module helps:

- To make the Supplier Questionnaire on level of cyber defense in the economy accessible online through the Directorate's website - <https://grc.cyber.gov.il>.
- To constitute a platform for suppliers to produce reports for declaring their level of compliance with the cyber defense requirements of this Methodology, as well as the ability to manage shortcomings arising for suppliers' during the remediation process. Furthermore, suppliers may update their details in the system at any given moment and a new ranking will be produced for the product/service accordingly.
- To make accessible a list of suppliers in the economy that have completed the certification process in conformity with the national methodology in this regard (suppliers and certified inspectors). Every organization in the economy will be able to perform a search in the system and receive a suitable breakdown of suppliers meeting the threshold risk defined by the organization. Based on this information, organizations can choose the most suitable supplier and sign an agreement with it to ensure the supplier's adherence to the defined risk level.
- To make accessible technical and methodological support through the Directorate's support center website and by calling 119.



Cyber Israel

Prime Minister's Office
National Cyber Directorate

Appendix D

THE REGULATION MODEL





- 1 **The Accreditation Body (AB):** The regulation and certification model adopted by the Directorate after analyzing models in Israel and internationally places the National Cyber Directorate at the top as an Accreditation Body. In this capacity, the Directorate is responsible for setting and maintaining appropriate professional standards. The National Cyber Directorate will serve as an AB whose role is to ensure that the certification bodies are indeed taking action to train inspectors and certify suppliers according to the requirements. The Directorate will also serve as a supervisory and control body that ensures from time to time that its requirements are being met. The regulations will change periodically.
- 2 **The Certification Body (CB):** These bodies currently operate in conformity with accepted international standards, perform reviews, training and certification using the variety of ISO management standards. Under these circumstances, the CBs will be required to comply with the particular requirements of the AB and will subsequently receive express authorization to operate on the AB's behalf within the requested scope - in our case, for example, this is the supply chain.
- 3 **The Inspection Body:** Bodies that perform inspections on behalf of the CB. An inspection body may be an organization or part of an organization; i.e., a specific professional in an organization. In our case, this refers to an inspector of the compatibility of the cyber defense measures of a supplier in an organization's supply chain, who verifies compliance with the conditions defined by the Directorate, which will be specified later (hereinafter: "the Inspector").
- 4 **Suppliers:** Suppliers wishing to complete the certification process and receive certification as complying with the requirements and processes within the scope of their application for certification, according to the requirements defined by the Directorate.



CB	Request to receive requirements in order to prepare accordingly
Certified inspector	Request to schedule an audit
Certified inspector	Physical audit is performed at the supplier's site / "supplier review"
Certified inspector	Completion of report of the audit findings
Professional advisory committee	Discussion of the report findings and decision-making
CB under Directorate supervision	Certification; supervision; maintaining qualification

5 Regulation levels

- Inspecting the cyber defense compatibility in an organizational supply chain constitutes regulation engaging in a relatively narrow scope and in direct correlation to suppliers serving in the supply chain of the organizations in the economy.
- This regulation was formulated in light of the insights whereby suppliers suffer numerous cyber incidents that may impact consumers of the services they provide (including major industrial organizations, banks, etc.), mainly due to the fact that suppliers' cyber defense capabilities are not the same as those of the organizations consuming their services.
- Considering the advantages outlined in the introduction, the Directorate expects organizations to instruct their various suppliers to take part in the process, including the receipt of a response from the supplier/inspector on its behalf to the Supplier Questionnaire according to one of the three levels of regulation and according to the level of risk that the supplier poses to an organization.
- Before explaining the levels of regulation, we wish to clarify that the highest level of regulation (A) is assigned to material suppliers. The definition of level A can be found in a comprehensive document issued by the Directorate entitled: "Defense Doctrine - Supply Chain."

"Material/critical supplier: A supplier that provides services such as: information systems support and/or maintenance, storing of sensitive information off the organization's premises, technological outsourcing services, etc. (Proper Banking Practices 363 - Managing Cyber Risks in the Supply Chain, clause 7), or a supplier when damage to it is liable to cause material damage to the customer. The decision about defining a supplier as material is at the organization's discretion. An exception to this is when a regulatory authority has defined in advance for organizations in the economy over which it is responsible that a particular supplier, or any supplier that meets defined criteria, constitutes a material supplier in any event."

- Below are the levels of regulation from the lowest level (C) to the highest level (A):
 - Self-assessment level - C: The supplier or any party acting on its behalf completes a self-assessment questionnaire and then signs a declaration. The report obtained can be exported to organizations with whom the supplier wishes to contract, so that they can receive an indication of the supplier's compliance with the relevant control standards.
 - Self-assessment level - B+: Completing a questionnaire and submitting evidence of implementation of the control. In this case as well, the supplier obtains a report that can be exported, along with the evidence required to substantiate its compliance with the relevant controls.
 - Level A: Intended for suppliers defined as material/ critical suppliers for an organization. This regulation level includes the two previous stages, which are carried out during a physical audit by an inspector on the suppliers' premises. This process is called a "supplier review" and constitutes a suitable control by an objective, third-party professional who personally examines the supplier's compliance with said requirements.
- At the conclusion of this stage, the inspector will submit a report of his findings during the inspection of the supplier to the certification committee, as specified below and, if the report shows compliance, a suitable certificate will be issued to the supplier and its details will be published on the Directorate's website and on the website of the certification body as a "certified supplier" (subject to the supplier's consent) or, alternatively, a report of the shortcomings will be issued to the supplier; these shortcomings must be rectified as a precondition to receiving the requested certification.

Inspection levels

A	  	Completion of a questionnaire by an independent inspector during a physical audit on the supplier's premises - "supplier review" Outcome: report and certificate
B	 	Self-Assessment + submission of evidence of implementation of the control/regulation Outcome: supplier declaration + evidence
C		Self-Assessment Completion of a self-assessment questionnaire, and the supplier signs a declaration Outcome: supplier declaration



6 Management of the requirements from the professional bodies in the regulation model

- **National Cyber Directorate** will assume a professional role, manage the process of controlled regulation and supervise the processes that it has outlined with the objective of maintaining a highly professional cyber defense standard.
- **Certification Bodies:** The training and certification activities defined by CBs require compliance with criteria defined by the Directorate in this regard:
 - Training bodies are required to prove:
 - active and continuous commitment in the management of a training center, inclusive of all of its advantages, staff, building, instrumentation, computer laboratory, platform and training process development and management, etc., which are regularly available to them for the purpose of current management;
 - focused commitment to technological training;
 - more than five years of experience in providing training in cyber defense topics will be considered an advantage.
 - Certification bodies are required to maintain the following certifications and capabilities:
 - valid certification under ISO 17021 - Requirements for Certification Bodies;
 - valid certification under ISO 27001- Information Security Management;
 - proven focused commitment to standardization for more than five years.
 - Inspectors are required to maintain the following certifications and capabilities:
 - Cumulative experience of at least five years in cyber defense in business companies;
 - Course completion certificate in data security/cyber defense representing at least 250 hours or recognized international certification such as: CISSP, CISO, CISA, CISM;
 - Familiarity with cyber defense technologies and products and with secured network topologies;
 - Know-how and experience in risk analysis and management;
 - Written and oral communications skills;
 - Significant presentation skills, including the handling of objections;
 - Hebrew - native language; English - proficiency;
 - Admissions committee;
 - Independent learning prior to the course;
 - Hands-on experience in cyber defense of more than three years in an established business organization is an advantage.

7 Management of the roles of the professionals in the regulation model



- **Roles of training bodies**

- Training bodies complying with the aforementioned requirements and responding to the public appeal to be announced by the Directorate will be required to provide a set of training services and to constitute an examining body according to the professional requirements of the Directorate, which issues a completion certificate to participants for the role for which they received training, and to maintain their qualifications, including through seminars, etc.
- Representatives of the National Cyber Directorate will sit in as active participants in training courses in order to comment and offer insights on the process, improve the methodology, improve the syllabus and the professional content provided by the Directorate, assess the lecturers, customize course assignments given to the participants, act as assessors of the training bodies' processes and operations, and provide immediate responses relating to the new methodology. They then report to the relevant professionals in the Directorate with a list of recommendations for additions, amendments, revisions and improvements, and analyze and correlate between the material being taught and the actual commencement of the work, such as an inspector of the compatibility of an organizational supply chain.
- The following are some of the Directorate's requirements with regard to the roles of a training body:
 - Marketing and advertising of training courses, webinars, dates of admissions committee meetings and all related publications;
 - Screening of candidates according to the threshold requirements defined by the Directorate;
 - Conducting entrance examinations and admissions committee meetings accordingly;
 - Training professional instructors according to the Directorate's requirements and course-building according to the Directorate's specifications/methodology for the required regulation.

- Conducting training courses and intermediate and final examinations (theoretical and practical-laboratory exams and simulations);
- Collecting payments for training courses and/or examinations;
- Providing facilities for the training courses (including a computer laboratory) and the certification examination (allocation of a designated physical location for holding the examinations);
- Preparing examinations (managing a team of exam preparers), scheduling the exams, managing them, assigning proctors to supervise during examinations, handling appeals and exceptional cases, and having responsibility over an updated database of questions;
- Issuing periodic reports;
- Issuing qualification certificates (subject to the approval of the Directorate's approval committee);
- Conducting a periodic review of the graduates' activities;
- Maintaining the graduates' qualifications, including the required refresher courses.



• Roles of inspectors

- Candidates who meet the admission criteria, successfully complete the required training course and pass the final examination shall be issued a suitable certificate from the training body and the National Cyber Directorate, subject to the approval of the Directorate's approval committee. The certificate must specify the version of the Directorate's Supplier Questionnaire for strengthening the supply chain that was the subject of the training.
- The inspector's details will be published on the Directorate's website as an inspector who has met the Directorate's requirements for inspectors of the compatibility of cyber defense for an organizational supply chain, subject to the inspector's written consent on the certificate.
- Inspectors must maintain their qualifications for this role by participating in seminars and continuing education courses, because the methodology being taught in the training courses (the version of the questionnaire, as stated above) is periodically updated, which is essential to performing this role and which will constitute a condition for maintaining the inspector's eligibility to have his details published on the Directorate's website.



- The production of the said seminars is the responsibility of the training bodies according to the Directorate's requirements and directives regarding the professional content to be taught during seminars.
- An inspector's role is to perform an analysis of materiality on the premises of the supplier that contacted him and wishes to receive the Directorate's recognition as a material supplier at the rank of A within a particular scope.
- "Analysis of materiality" means: conducting inquiries and investigations, reaching independent impressions of the supplier's systems, receiving evidence that must be examined during the audit, conducting examinations in the various departments, holding conversations with professional employees regarding the relevant control, examining the security measures in the server room, inspecting physical security measures, reviewing rules in FW, querying about access controls, examining policies and procedures, authorizations by the board of directors and the management, etc..
- There are six possible inspection topics in the Supplier Questionnaire: (1) general, which includes all of the controls in the Supplier Questionnaire; (2) handling of information; (3) remote access; (4) work performed on a customer's premises; (5) secure software development; (6) cloud-based information storage.
- The customer ordering the inspector's work will define the topic of the audit on the supplier's premises that it is ordering.
- The subjects taught during the training course that inspectors must successfully pass prior to beginning work include: the details of the audit of each control, the extent of its implementation in the supplier's systems, the evidence that must be attached to substantiate the supplier's compliance with the relevant control, the inspector's work on the Directorate's online system, the organizational goals and controls system - the Supply Chain Module, the mode of completion of the report of the findings, handling objections, legal aspects, the world of auditing, etc..
- The inspector will prepare a report of the findings during the inspection of the supplier and will attach requisite evidence as needed.
- The inspector will enter full details about every control in the appropriate field and for every instance of an entry of "irrelevant," will be required to include maximum details that will satisfy the certification committee that the specific control is indeed irrelevant to the supplier or the sector of activity under inspection.
- The mode of submission of a supplier's file to the certification committee is specified below in clause 12.7.3, "Roles of certification bodies".
- Inspectors must be free of conflicts of interest and submit reliable reports. When submitting supplier files to the certification committee, inspectors must submit declarations of compliance with the aforementioned in relation to every supplier inspected.
- Inspectors must regulate their agreements with suppliers that hired their inspection services by way of a legal document safeguarding the confidentiality of the items to which they are exposed during inspections.
- The Directorate recommends that all inspectors protect themselves for the term of their agreements with suppliers by purchasing professional liability insurance with coverage suitable for the provision of services of this type.



- **Roles of certification bodies**

- Certification bodies meeting the aforementioned requirements and responding to the Directorate's public appeal will be required to provide end-to-end certification services, from the stage of hiring suitable certification functions encompassing all of the Directorate's professional requirements until the certification is issued to approved organizations [sic - should be suppliers?], close supervision of the suppliers, verification of the reliability of the data and ensuring that suppliers continue to qualify for certification.
- **Certification manager**
 - Will be responsible for examining the customers' [sic - should be suppliers'] files, which include a report of the inspector's findings and the evidence required, and for ascertaining whether they meet the standards specified in the specifications/the Directorate's methodology as a professional body;
 - Will be hired by the certification body and will not have any claim that he/she is employed by the Directorate;
 - Will be an individual professional possessing certificates and reliable evidence of his/her knowledge, experience and qualifications according to the following requirements:
 1. Clearly technological education, which includes a degree in software engineering or computer science;
 2. International certification (CISO/CISSP)
 3. Clearly technological qualifications and hands on experience in cyber defense reflected by professional seniority and experience of more than five years;
 4. Familiarity with technological tools and products;
 5. Familiarity with cyber auditing aspects;
 6. Background in certification; extensive familiarity with international accreditation and activities in this regard.
 - The certification manager's appointment percentage will be defined by the certification body, provided that the certification body does not compromise the duration of the examination and provided that the examination date does not exceed 14 business days from the submission date of an application to certify a supplier.



o **Content expert**

- **Background:** In instances in which the supplier undergoing certification engages in particularly technical spheres of business, such as a supplier of fintech equipment and instrumentation or a designated supplier to defense entities, etc., and the involvement of a specific content expert is needed for the purposes of examining the report of the findings and the evidence submitted, a content expert will be added to the certification committee according to the Directorate's recommendation or, alternatively, an expert proposed by the certification body, provided that the expert is acceptable to the National Cyber Directorate.
- **Details of the process:** The content expert, who shall be invited to advise the certification officer, will be selected according to a list of the service categories and relevant content experts that the Directorate shall issue to the certification body, and which shall be updated from time to time.
- **SLA:** the timeframe for decision-making with regard to the relevant supplier, in the event that a content expert is also required - is 21 business days as of the submission date of the supplier's application for certification. The timeframe for issuing a certificate to a supplier is a maximum of seven business days after the decision regarding the supplier has been reached.
- **Decision-making:**
 1. In case of agreement between the certification officer and the content expert, the judgment of the Directorate's representative will be optional.
 2. In case of disagreement between the certification officer and the content expert, the decision with regard to certification of the supplier will be ruled on by the Directorate's representative.
 3. To dispel any doubt, the ruling of the Directorate's representative will be a veto right and will be final with regard to certification of the supplier.

o **Submission of a supplier's file for certification**

- Submission criteria - a certified inspector who conducts an inspection with the supplier's permission and reaches the conclusion that the supplier fully complies with the required controls according to the desired scope of the inspection of the supplier, shall submit the supplier's file to the certification body.
- The supplier certification file must contain the following documents:
 1. A consent form signed by the supplier, whereby the supplier agrees to undergo inspection by the certified inspector, the supplier file is being submitted with its consent and the supplier consents to be included in the database of certified suppliers if it complies with the requirements of the inspector's declaration about the reliability of the information stated in the report of the findings and about the absence of any conflicts of interest between the inspector and the supplier that is the subject of the file submitted.
 2. The report of the findings regarding the supplier completed by the certified inspector in the Organizational Goals and Controls System as a PDF file, which must be signed (handwritten or digitally) by an authorized representative of the supplier.
 3. Cover page listing the evidence required to prove compliance with the controls.



4. Reporting table regarding the scope of the inspection performed on the supplier, which is the subject of the report, which will include the minimum hours required for the scope of each inspection.
 5. Confirmation of payment for the cost of the inspection and the supplier certification, according to the certification body's rates.
- **Mode of submission:** Either submission of a hard copy to the certification body or in a DOK or, alternatively, via e-mail to a designated inbox of the certification body in a PDF file containing the entire supplier file.
 - **Alternative mode of submission of evidence:** Suppliers that do not wish to forward the full file of evidence to the certification committee are given an alternative whereby the certification committee's examination of the supplier's compliance with the desired scope of inspection will be carried out on the supplier's premises or at his address for service.
 - The supplier is responsible for presenting all required evidence to the committee that was presented to the inspector and served to convince the inspector, according to the report of findings submitted to the committee.
 - The visit by the certification manager and, if necessary, the content expert, to the supplier's premises for an independent impression of the evidence specified in the report of the findings, according to which the inspector reached his/her conclusions, involves an additional cost resulting from the travel expenses, etc. according to the rate to be published by the certification body.
 - Insofar as it will become necessary to submit additional evidence or detailed explanations, the inspector will be invited to a face-to-face/telephone meeting with the certification body and will be required to provide suitable responses to the certification manager and/or to the content expert until they are convinced of the supplier's eligibility to be certified as an approved supplier, or, alternatively, regarding the immediate rejection of the supplier's application.
 - **Rectification of shortcomings:** Insofar as the certification manager's examination may reveal unreasonable shortcomings relating to the classification of the supplier as a material supplier, the implementation of a control that is not commensurate with the level of security required due to the supplier's sphere of business, the completion of an unsatisfactory report due to the absence of technological means required for that supplier or due to a concern about reliability, etc., the supplier's file shall be returned to the inspector, without certification, while specifying the shortcomings requiring rectification, with a deadline for re-submission not exceeding 90 days. The re-examination of a supplier's file involves an additional payment at a reduced rate, according to the rate to be published by the certification body.



- **Certificates**

- The certification manager's approval of the report of the findings submitted by the certified inspector according to the required evidence that was submitted, is tantamount to approval of the supplier's certification for the scope submitted in the application.
- Supplier certification will be in effect for two years as of the date of its approval by the certification manager as a certified supplier. At the end of the first year of the supplier's certification, the supplier or any delegate on its behalf is required to submit a declaration signed by an authorized representative that no material changes have occurred in the scope of the examination that resulted in its certification and that it undertakes to give notice of any change, so that the certification issued to it will remain in effect for an additional year and so that its name will not be removed from the database of approved suppliers.
- Certificates will be issued to suppliers by the certification body, subject to the Directorate's approval of their contents and according to the sponsorship clause in the agreed regulations.

- **SLA summary of certification aspects**

- The certification manager's appointment percentage will be defined by the certification body, provided that the certification body does not compromise the duration of the examination and provided that the examination date does not exceed 14 business days from the submission date of an application to certify a supplier.
- The time frame required for decision-making with regard to the relevant supplier - is 21 business days as of the submission date of the supplier's application for certification; in the event that the opinion of a content expert is also required, it shall be 28 business days as of the submission date of the supplier's application for certification.
- The period for a supplier's rectification of shortcomings will be limited to a time frame not exceeding 90 calendar days from the date of the notice to the supplier and until the re-submission of its application.



- The time frame required to deliver a certificate to a supplier from the date of the decision on its file shall be a maximum of seven business days.
- A supplier's appeal of an application rejection or a partial rejection in its case will be discussed with a representative of the Directorate within 14 business days of the submission date of the supplier's appeal.

- **Certification rates - summary**

- The certification rate shall be priced by the certification body and shall be approved by the Directorate for the purposes of providing thorough and professional service on the one hand and, on the other hand, maintaining a reasonable and proportionate cost that will not impose a burden on the economy.
- The basic certification rate will be in the form of an examination fee by the certification manager, calculated based on the scope of the examination performed for the supplier, and a separate cost for issuing and delivering the certificate to the supplier.
- A separate fee for examination of the supplier's file by a content expert, if necessary.
- A reduced rate for re-examination/additional review after the supplier resubmits its file after having rectified shortcomings identified as a result of the original inspection.
- Rate for physical inspection with the supplier's permission, for a supplier not wanting evidence to leave its premises and requesting the certification manager to obtain an independent impression at the supplier's premises.



Cyber Israel

Prime Minister's Office
National Cyber Directorate

Appendix E

SAMPLE AGREEMENT*

* Control 16.2 - Cyber Defense Methodology for Organizations.



1. The supplier must comply with the provisions of the regulations / law / standards in effect for its business sector throughout the entire term of the contract.
2. The supplier undertakes to comply with the supply chain requirements of the National Cyber Directorate - Supplier Questionnaire (Appendix B to this document). The scope of the inspection and the mode of proving compliance with these requirements shall be according to the organization's definition (one of the three levels specified in this document - A, B or C).
3. The supplier shall identify a contact person who shall serve as the cyber defense liaison vis-à-vis the organization's relevant activities, whose identity, particulars and contact details shall be approved by the organization.
4. All costs relating to the information security of the systems, information security solutions and databases shall apply solely to the supplier.
5. The supplier must report in writing about operations that are intended to serve various needs but constitute a security vulnerability in the connection, such as a user name and password backdoor used to open a locked account of the organization in the event that the password is forgotten. If no operations of this type exist, then the supplier must submit a declaration that no such operations exist, to the best of its knowledge.
6. Information security risks, cyber defense risks, i.e., databases and systems connected to the internet or to public communications networks, are exposed to a wide variety of internal and external risks. The sensitive information contained in the project's [sic] database requires the supplier to maintain stringent cyber defense mechanisms. The supplier must make use of all of the technological means and the procedures required to prevent - at the very least - the creation of the following risks:
 - Leaking and exposure of information: An information leak is defined as a forwarding of information between the supplier's system to any unauthorized third party. The supplier must implement a DLP system⁸ to prevent information leaks. The system must cover all channels used to send information from the organization.
 - Denial of service⁹ The supplier undertakes to institute the measures needed to detect and neutralize incidents of denial of service.
7. **Privacy protection, confidentiality and warranty**
 - The organization is the owner of the databases. The supplier is absolutely prohibited from selling, transferring, or fully or partially copying (whether

⁸ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 5.1.

⁹ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 9.3.



a hard copy or digital copy) any information belonging to the organization without the organization's prior written consent.

- The supplier undertakes that it shall use information solely for the defined activities and not for any other activity.
- The supplier shall sign a confidentiality agreement as required by the organization and shall require each of its employees involved in the performance of the services to sign it.
- The supplier shall forward information in a secure format by using the secured information-transfer means approved by the organization.
- **Data encryption¹⁰**
 - Data at rest - the data stored in the system must be encrypted at a minimum strength of Advanced Encryption Standard AES-256.
 - Data in transit - all information in transit must be encrypted using TLS or IPsec with a key at a minimum length of 128 bits.

- **Secure development¹¹**

The supplier undertakes that if software development is being carried out, all of the developments will comply with the customary principles for "secure development." The supplier of the system/application key to the organization is required to present a report on the performance of a code review and a penetration test by an external company.

8. Physical protection¹²

- Any physical location in which information relating to the organization is being managed must be secured using physical means of protection (entry control system, cameras and control means existing on the market), and entrance to the site must be restricted solely to authorized personnel, on the basis of the need for information.
- The supplier shall be required to separately define security procedures at its various facilities in which the information is used within the scope of this agreement.
- The supplier must store all material coming from the ____ system in a room that is filmed and monitored 24/7 and will present investigative capability of at least two weeks retrospectively.

9. Documentation¹³

For the purpose of investigating incidents and for control capabilities, the supplier must maintain technical documentation of the telephony systems and network components. The control channel (such as log files) must be retained for a time frame to be defined between the supplier and the

¹⁰ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 8.

¹¹ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 17.6.

¹² As per the Cyber Defense Methodology for Organizations, section 6.2, ID 18.

¹³ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 21.



organization and, at the very least, as required by law and by customary standards in the field.

10. Monitoring¹⁴

The supplier must document user operations in a system/access of the databases, which shall include the user's identity, the date of the operation, the details of the operation, etc. The supply shall monitor and detect abnormal patterns of activity in the system and by users, including, inter alia, consumption of resources, data extraction, and activity at abnormal hours.

11. Recording

The supplier must record activities being performed in a system. This recording must be retained in the systems for at least thirty days. The recording will be carried out at the level of _____ (to be defined according to the nature of the agreement).

12. Backups¹⁵

The supplier must perform daily / weekly / monthly / quarterly backups (select the desired frequency). The supplier must institute procedures for data recovery and restoration for situations of an operational failure and/or data security failure and perform quarterly drills of back-up data restoration to verify the good working order of the backups.

13. Hardening of components¹⁶

The supplier must harden communications equipment, infrastructure, applications (servers, routers, switches, terminal workstations, databases, its sites, etc.) according to the Best Practices documents for each software and hardware manufacturer.

14. Workstation connection and remote connection to the organization's network

- A health test must be performed for workstations as a precondition to connecting them to the organization's network (which shall include: verifications that an authorized anti-virus program and the operating system have been updated with the critical security updates).
- The connection must use a secure communications channel, such as IPSEC or SSL-VPN, with the legal external IP address that has been approved by the organization.
- Remote connection to components defined as "end of life" by the manufacturer must be prohibited.

15. Human resources¹⁷

¹⁴ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 21.

¹⁵ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 25.10.

¹⁶ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 6.1.

¹⁷ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 19.



Users and user authorizations in the system must be handled according to the following principles:

- The management of user access authorizations shall be determined according to the job definition.
- Compartmentalization of users of the system and display of solely relevant information.
- Maintenance of an updated list of officials and defined access authorizations.
- Employee screening and vetting.
- Training employees and increasing awareness about cyber risks, particularly employees with access to information on _____ (critical / sensitive system). The training must be a precondition to the supplier's employment of the employee for work relating to the organization.

16. Reporting, control and alerts¹⁸

- Reporting any indications of compromise or abnormality detected during the agreement to the personnel authorized to act on behalf of the organization.
- Immediate reporting (on the same business day) of abnormal incidents.
- Incident control and reporting to the organization

The supplier must implement procedures for handling data security incidents: alerts, recording and managing of the incident, escalation process and notification of a representative of the organization. The supplier further undertakes to report to the organization, both in writing and orally, immediately while the incident is occurring.

- During these incidents, the supplier must enable investigative activities, such as forwarding relevant log files, duplication of servers and workstations, the opening of encrypted communications channels for the purpose of reviewing them, etc.
 - Reserving the right to audit
- The organization or any party acting on its behalf is allowed to perform a data security audit at any time without warning or advance coordination with the supplier.

17. Password management¹⁹

The supplier must implement identification on the basis of a password that will comply with the following password policy:

- Use of 8 characters comprised of at least three different variables - capital letter, small letter, numeral, special character.
- Previous passwords may not be reused.

¹⁸ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 24.4.

¹⁹ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 4.35.



- After three failed attempts, the user must be locked out.
- Passwords must be changed at a frequency of at least once every three months.

18. Outsourcing²⁰

- The supplier shall not make use of the services of any third party for material service operations that are part of the provision of the service that the supplier is providing within the scope of this agreement, without the organization's prior written authorization.
- The supplier must analyze the data security risks involved in contracting with external parties and must submit a report of its findings to the organization and its plan for rectifying shortcomings.
- If outsourcing is necessary and the outsourcing party is approved by the organization, the supplier is responsible for ensuring that all of the data security provisions specified in this document are also being implemented by the external party.

19. Completion of service and deletion of data.

- The supplier undertakes to enable the organization to terminate the service at any time without any unreasonable contractual restrictions and undertakes to export the information so that it may be restored to another system within five days of the organization's notice.
- The supplier undertakes to block the user accounts and the access authorizations after end of use.
- The supplier undertakes to delete all system components and all stored information (hard copies, soft copies, hardware, storage means, documentation, etc.) upon the termination of the service, and to provide proof to the organization of the mode of execution of the deletions.

²⁰ As per the Cyber Defense Methodology for Organizations, section 6.2, ID 16.