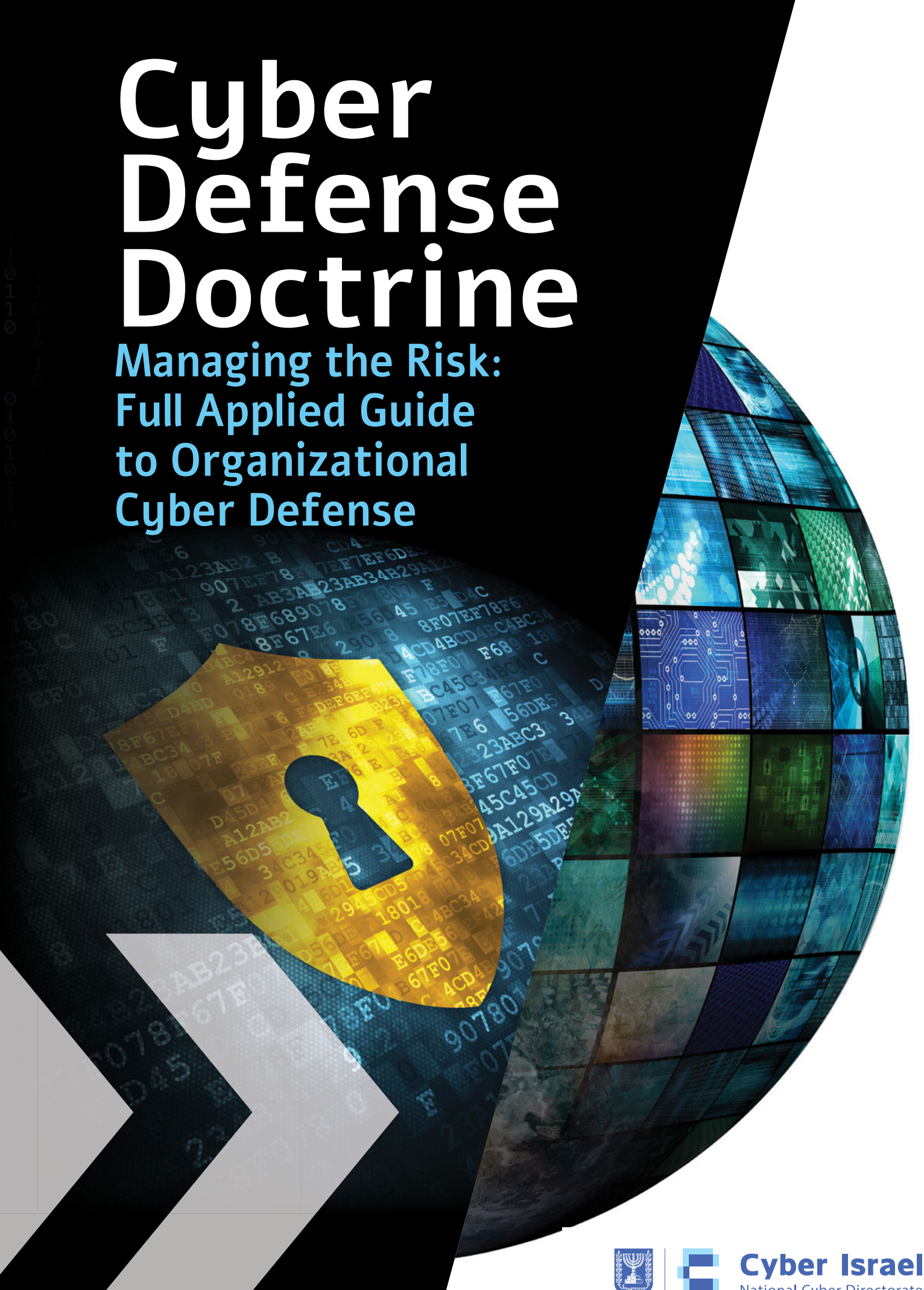
Cyber Defense Doctrine

Managing the Risk: Full Applied Guide to Organizational Cyber Defense



Cyber Israel
National Cyber Directorate

Cyber Israel
National Cyber Directorate

Managing the Risk:
Full Applied Guide to Organizational Cyber Defense
(Cyber Defense Doctrine 2.0)

June 2021

Table of Contents

Cyber Israel
National Cyber Directorate

INTRODUCTION

Dear managers and experts in the fields of information security and Cyber Defense, Cyberspace is the outcome of technological advancement, connectivity and a global connection engagement with.

The growing dependence on cyberspace heralds an era of technological innovation and tremendous developments for man and his environment. But alongside these, a space of threats is developing, which affects the organizational functional continuity, the integrity of the manufacturing processes and the confidentiality of organizational information.

Cyber attacks can harm organizations and even lead to the cessation of production processes, economic damage and damage to reputation.

The State of Israel is making a national effort to protect the civilian cyberspace.

The Organizational Defense Doctrine is a constituent element of the National Cyber Security Strategy, which consists of various layers of Defense for the Israeli economy and its functional continuity.

The Organizational Defense Doctrine sees the organization as a whole and enables the raising of the level of organizational resilience through the continuous assimilation of processes, methods and Defense products.

The application of the Organizational Defense Doctrine will improve organizational resilience to cyber attacks.

EXECUTIVE SUMMARY

The purpose of the Defense Doctrine is to present to the Israeli economy an orderly professional method for managing cyber risks in the organization.

Using the method presented in this document, the organization will recognize the risks relevant to it, formulate a defensive response and implement a risk reduction plan accordingly.

Step A – Identifying to which category the organization belongs:

- **Category A** – Organizations with medium-to-low potential for damage as a result of a cyber incident.

- **Category B** – Organizations with a high potential for damage as a result of a cyber incident.

A categorization questionnaire appears on page 7.

Step B – Perform a risk assessment and management process

Cyber Defense activities are carried out due to the organization's desire to manage the cyber risks to which it is exposed.

For this purpose, the organization will first define what its main Defense objectives are (usually business processes or digital assets), what level of Defense is required and what are the Defense gaps compared to the desired situation, and then proceed to build a work plan to minimize the gaps.

This process is carried out differently in different organizations, depending on their size, compliance with legal and regulatory requirements, and other parameters.

This document presents a number of methods for risk assessment and management, differentiating between organizations with relatively small potential for damage (up to USD 1.5 million) and organizations with greater potential for damage – for which an extended methodology has been developed.

The final product after working with this document

The organization will understand the organizational risk map, and what controls are needed to reduce those risks – including the right priorities for implementing the work plan.

These controls will form the basis for building the work plan, allocating resources and preparing the organization accordingly.

1 PREAMBLE

Cyberspace constitutes an integral part of our daily lives. On a personal level, we search for information on the Internet, find our way on the road using navigation software, talk on cellphones, and some of us even have a pacemaker or insulin pump connected to the Internet – and they are all part of Cyberspace. On the business level, we use credit cards, manage a customer database, manage a global organization through computer networks, market, buy and sell – all while relying upon Cyberspace.

For many of us, available, accessible and reliable Cyberspace is a necessary condition for conducting our daily lives – especially when it comes to conducting business. It is easy to understand this when these are denied from us temporarily. How do we run a business without a cellphone? Without the knowledge stored in the corporate network? Without credit card clearance capability?

In Cyberspace there are options and opportunities on the one hand, and threats and risks on the other hand.

In the Cyber realm, there is extensive activity of state espionage, industrial espionage, organized crime and occasional crime. All of these may affect national security (for example, by inflicting damage on critical national infrastructure, such as the electricity or water systems, through Cyberspace) or business conduct (for example, through commercial espionage or economic blackmail).

Today, different organizations protect themselves against these threats in different manners. There is a lot of information on the Internet about ways to protect against cyber risks, and it consists of a collection of orderly methodologies, best practices, "do's and don'ts", and more.

Many organizations in Israel and around the world struggle with questions such as "Are we investing enough in Cyber Defense?", "Are we investing properly in Cyber Defense?" or "Are we investing in Cyber Defense in accordance with what is common in our economy or industry?"

The Defense Doctrine presented in this document shall assist organizations with mapping out Cyber risks, understanding the organizational significance of risk realization, and defining proportionate safeguards to mitigate major risks.

The Defense Doctrine is accompanied by various aids, which will help the organization to adopt it easily. They include professional supplements, Cyber Defense procedures and recommendations for implementation for various areas, procedures applicable with respect to Israeli legislation and regulation and international standardization, computerization of the Defense Doctrine through a convenient technological platform – and more. All the latest information appears on the website of the Israel National Cyber Directorate:

https://www.gov.il/he/departments/topics/organization_cyber_protection

2

PRINCIPLES OF DEFENSE DOCTRINE

The main principle of Defense Doctrine is defense against relevant threats – that is, to recognize that when it comes to protecting the continuity of the organization's functioning, its assets and its objectives, it must be based on understanding the referential threat, and on the intelligence and changing trends in the relevant field.

This principle is expressed through the following sub-principles:

A. Management responsibility

The responsibility for protecting the information lies first and foremost with the management of the organization.

B. Defense from the Adversary's View

The weight of the Defense recommendations, as well as the definition of priorities for their implementation, are derived directly from understanding the common attack scenarios and the effectiveness of the Defense recommendations against them. The Defense recommendations are the means of achieving organizational resilience, in accordance with the threats and ways of action relevant to the organization.

C. Defense based on Israeli knowledge and experience

The Defense Doctrine allows for a focus on the risks relevant to each and every organization. As part of the activities of the Israel National Cyber Directorate, periodic audits and intelligence assessments are carried out throughout the entire Israeli economy. These actions make it possible to target organizations in specific areas in the various Defense circles.

D. Defense in accordance with the potential for damage

The investment in protecting each Defense target in the organization will be in accordance with its level of criticality for the organization's functioning.

E. Defense based on depth of implementation

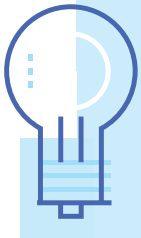
The Defense Doctrine allows the organization to implement controls at different levels of maturity on issues such as SOC, DLP or risk surveys. Thus, instead of looking at controls from the point of view of compliance only, the organization will examine them according to their implementation effectiveness. This is reflected in the definition of "depth of implementation" for each Defense (control) recommendation and the definition of "required evidence" accordingly.

3 THE STRUCTURE OF DEFENSE DOCTRINE

The Doctrine consists of two different tracks for risk assessment and management, which are derived mainly from the potential damage to the organization as a result of a cyber incident:

The track for a category A organization – intended for organizations that the scope of damage caused to them by a cyber incident does not exceed USD 1.5 million. This track includes a simple and quick process of mapping Defense objectives and answering a limited number of questions, which are tailored to organizations from this category. Usually, the process is carried out through an external party which accompanies the Cyber Defense aspects of the organization.

The track for a category B organization – Intended for organizations that the extent of the damage caused to them by a cyber incident may cost more than USD 1.5 million. This track includes a process of Risk Assessment, understanding the required Defense response to the Risk Matrix and Risk Appetite, examining the current situation in the face of industry-accepted Defense recommendations (Gap analysis) and formulating a work plan for the mitigation of risks (Mitigation Plan) or other risk handling measures. In most cases, the evaluation process and the implementation of its conclusions are led by a person in charge of Cyber Defense within the organization (by virtue of his position or of his responsibility in addition to his position). Sometimes an external party is responsible for this.



To check whether a cyber incident in your organization will cause damage amounting to more than USD 1.5 million, it is recommended that you consider, among other things, the following parameters:

- Loss of income as a result of disruption of business continuity
- The cost of handling the incident (including response teams, content experts and more)
- The cost of fully recovering information systems (including licensing, hardware and software)
- Direct cost deriving from violation of law/regulation and business claims
- Indirect damages, such as damage to reputation – including the impact on the loss of existing and new customers

In order to assess the damage more accurately, it is possible to use calculators and professional studies, which take into consideration parameters such as the sector in which the organization operates, the type of information and the amount of records held by the organization.

However, an organization should examine the potential for harm in a broader perspective, which involves aspects of corporate responsibility. The worldview underlying this approach is that the essence of the business organization is not only in creating profit for shareholders, but also in creating value for all stakeholders – customers, employees, suppliers, investors, the community and the environment.

Using this approach weighs the effects of a cyber incident on the stakeholders in the organization, strengthens mutual trust between them and the organization, and improves long-term economic performance. This approach includes addressing potential damage to human life, to public trust and to third parties, and a broad and comprehensive view of the aggregate damage – not only to the organization, but also to the wider circles of influence.

To quickly understand which category your organization belongs to, you can use the following rules of thumb:

Organizational classification tree – the chart below weighs a number of parameters, such as the size of the organization, the number of customers, the turnover and the dependence on digital technology. This tree is not a substitute for examining the potential for damage, but it may help guide the organization along its appropriate path:

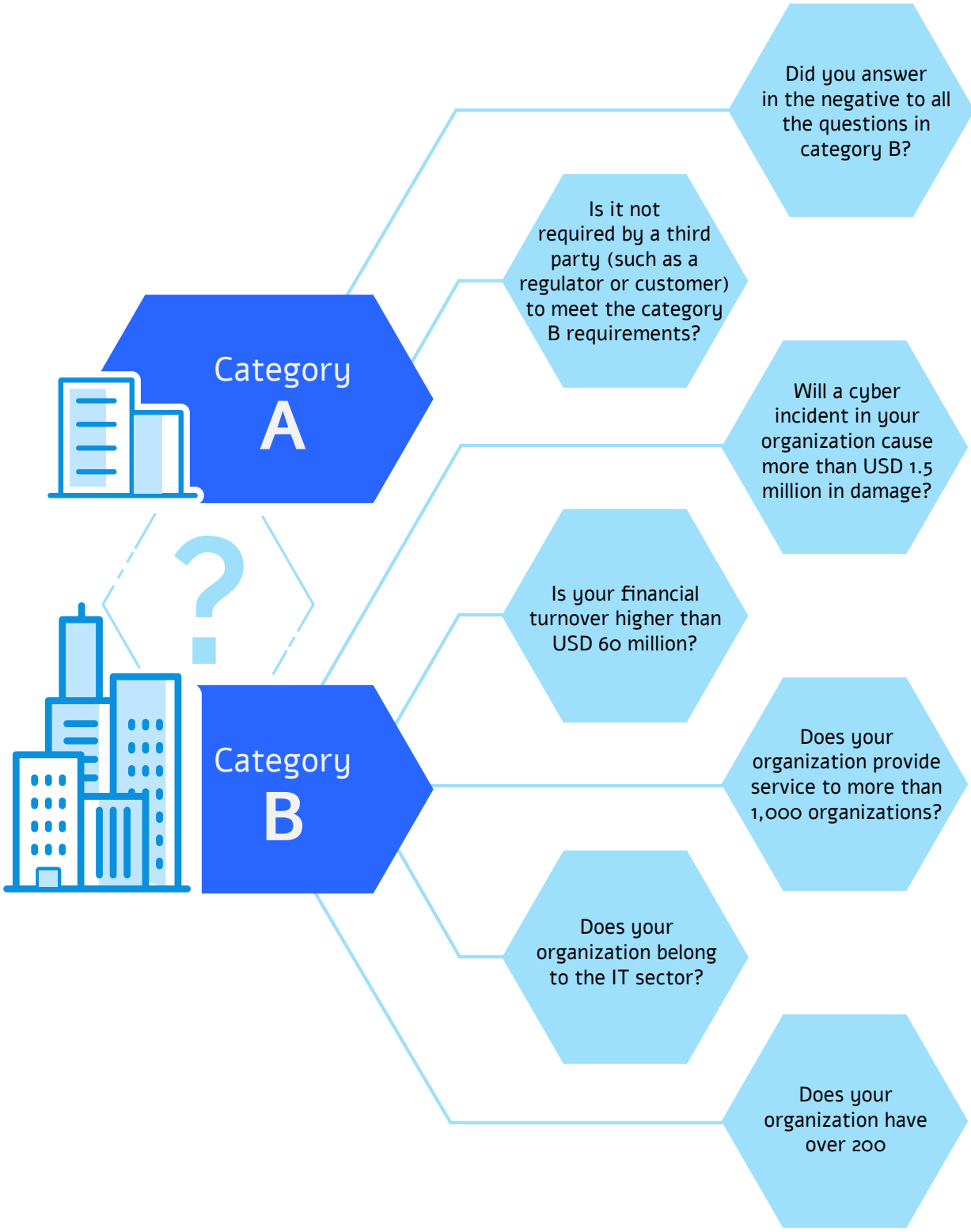
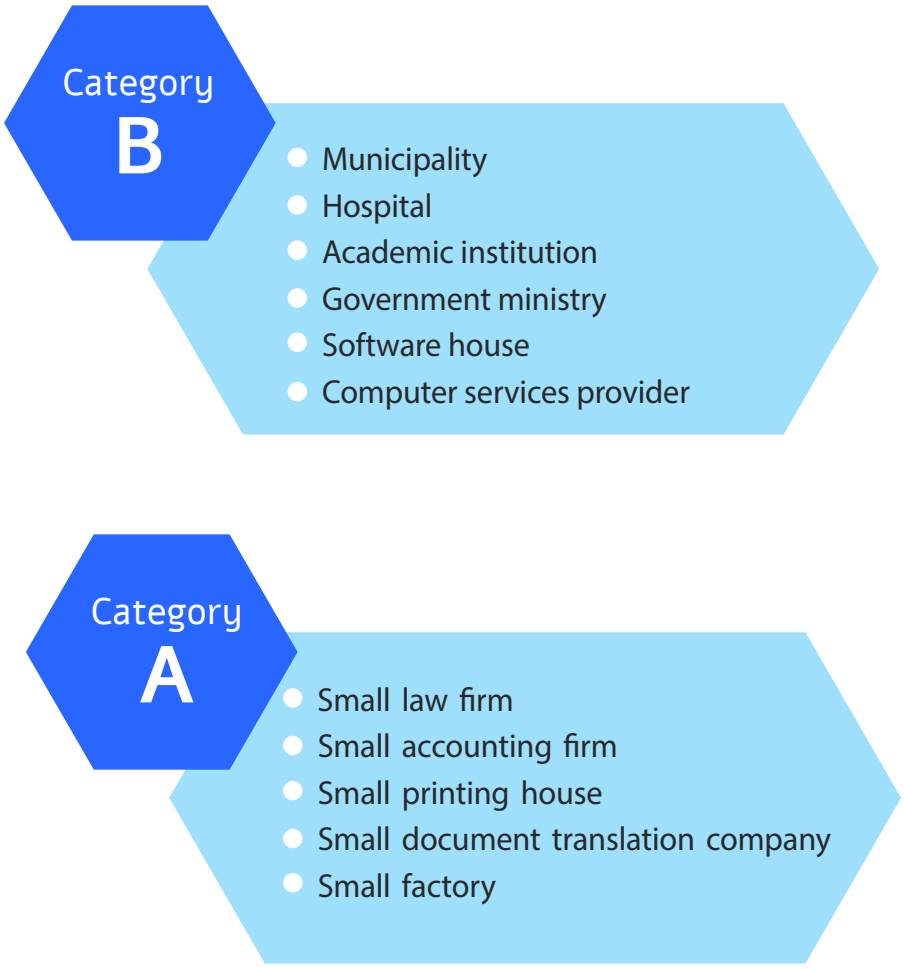

Category
A
Did you answer in the negative to all the questions in category B?
Is it not required by a third party (such as a regulator or customer) to meet the category B requirements?
Will a cyber incident in your organization cause more than USD 1.5 million in damage?
?
Category
B
Is your financial turnover higher than USD 60 million?
Does your organization provide service to more than 1,000 organizations?
Does your organization belong to the IT sector?
Does your organization have over 200

Table below shows a general example of a possible division of types of organizations into the categories recommended for them:

The above division is simplistic, and is intended to provide a preliminary rule of thumb for classifying organizations into different categories.



Questionnaire – Answering the following questions will help you decide which category the organization belongs to:

- **What is the motivation for attacking the organization?**
  - **What types of information exist in the organization?** For example, personal information, financial data (such as credit information), medical information, patents or security information.
  - **What is the scope of sensitive information available in the organization?** For example, are there hundreds of records, thousands of records or hundreds of thousands?
  - **What is the nature of the organization?** For example, is it a software house that might provides an penetration path for a potential attacker?; is it an organization that stores information of many customers? or is it one that is regarded as a national symbol?
- **What is the attack surface of the organization?** For example, the amount of the organization's open interfaces and their type, the global deployment and accessibility of the organization's digital assets or the amount of the organization's suppliers and their type.
- **What are the resources allocated by the organization to Cyber Defense?** For instance, is there a chief information security officer (CISO) in the organization; does the Information Systems Manager allocate resources to Cyber Defense; or does the organization's Cyber Defense budget fit the outline of threats in the sector, and was it defined by management to be a certain percentage of the annual turnover or of the IT budget?

If the organization incurs additional obligations due to legislation and/ or regulation that it must comply with, contractual requirements or various business needs – this may result in its transfer from category A to category B. In addition, organizations with a high dependence on technology, which may suffer significant damage as a result of a cyber incident, should consider carrying out the process in accordance with the requirements of category B.

4

THE PLANNING PROCESS IN THE ORGANIZATION'S VIEW

Working with this document according to the organizational categorization

For a Category A organization:

Identification of risks and their rating according to a number of parameters, with an emphasis on the potential for damage and the likelihood of its realization – or according to the weighting of the threats, vulnerabilities and their degree of relevance to the organization. At the end of this stage, the organization will have a rated list of risks that need to be addressed.

Identifying assets and business processes that are vulnerable to cyber attacks. At the end of this stage, the organization will have a list of defense targets. Advanced organizations will map business processes to defense objectives, while analyzing the interrelationships between business processes and relevant defense objectives

Reaching a decision about how to treat each of the risks.

Simultaneously with the implementation of the defined work plan, an initiated process of validation and re-examination must be performed from time to time. On the one hand, the process shall address new threats, research and cyber incidents; on the other hand, the organization's activity develops at the business and technological level (for instance, in the case of mergers and acquisitions, which affect the organization's infrastructure).

Formulation of a plan to raise the level of defense, so as to reach the desired level of risk – including an understanding of the nature of the exposure to risk if the required controls are not implemented.

For a Category B organization:

1 Demarcation of the activity – what should be protected?

- **1.1** Defining the scope of powers and limits of responsibility of the cyber defense party in the organization
- **1.2** Defining an organizational strategy for cyber defense
- **1.3** Demarcation of the risk survey

2 Risk assessment

- **2.1** Identifying relevant risks to the organization
- **2.2** Analyzing the risks
- **2.3** Risk assessment

3 Determining a strategy for risk treatment

- **3.1** Defining how the organization responds to risks that have been identified and analyzed

4 Building a work plan

Defining performance and control metrics/indexes, mechanisms, tools and a framework for controlling the development of threats and the progress of the approved reduction/mitigation plan

5 Continuous and ongoing audit and control

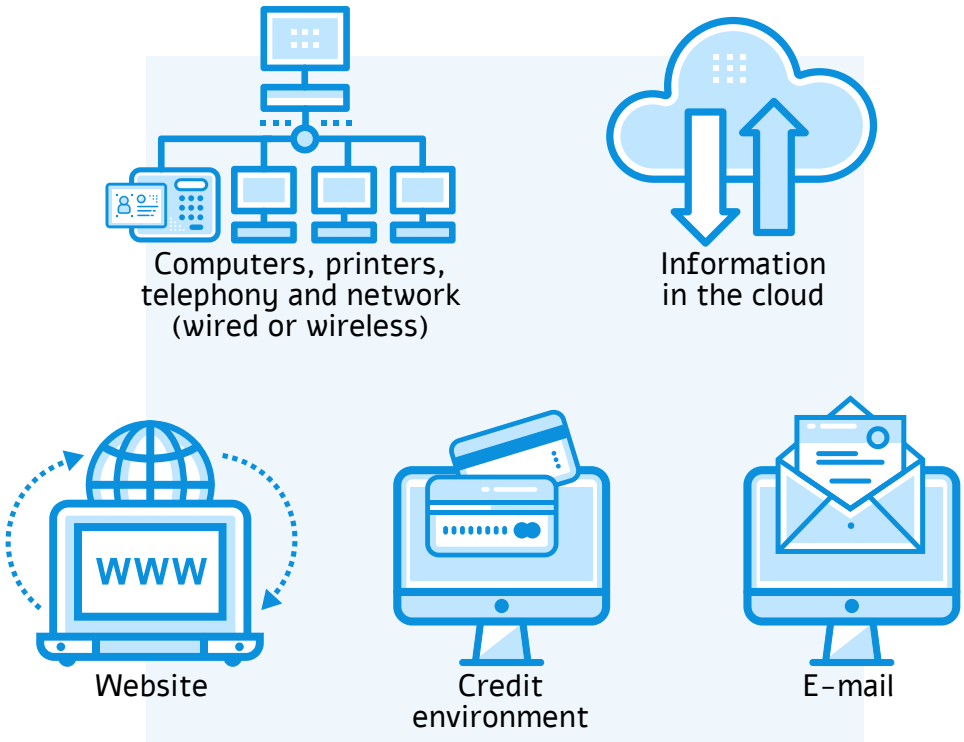
Defining performance and control metrics/indexes, mechanisms, tools and a framework for controlling the development of threats and the progress of the approved reduction/mitigation plan

4.1 | Implementation of the Doctrine of Defense for a category A organizatio

Stage 1: Mapping of the activity

Check with the technical support body the types of equipment and computing assets used by the organization. Understand what the organization's digital assets are and where they are stored. The purpose of this step is to understand the goals of Defense against cyber threats. As part of the demarcation stage, it must be understood whether the organization has databases, digital assets such as social networks, or organizational systems and software such as a payroll system, attendance system or payment and clearing stations.

At the end of this stage, the organization will have a list of assets,whose level of defense should be examined against cyber risks in accordance with the list of recommended controls.



Example of mapping Defense objectives in a Category A organization

Stages 2 and 3 : Assessing the risks and determining a strategy for dealing with them – the Ten Commandments for the organization in category A

A Category A organization needs to defend itself in a way that is appropriate to the potential for harm. Therefore, it must use extremely high-efficiency controls.

In many cyber incidents the attackers do not consider the size of the organization or the potential damage that may be caused to it. Many small businesses have experienced ransomware attacks, customer database leaks, customer information theft and more.

In order to reduce the chance of being injured in such incidents, and to increase the survivability and continuity of the business in the incident of an attack, it is recommended that each organization adopt the Horizontal Defense requirements set out in Appendix A of this document. These controls are divided into the following ten categories of defense:

1 Management Responsibility

Understand the risks lurking for the organization in cyberspace and build a work plan to close the Defense gaps in this area.

2 Malicious code prevention

Use malware handling technologies and make security updates to your organization's systems. In particular, care should be taken to protect against malware which arrive via email and by surfing websites

3 Encryption

Encrypt the remote connection of the organization's employees and suppliers, using simple and commercial encryption mechanisms. Encrypt access to sensitive information using an encrypted communication medium (both for surfing the organization website from a wireless home network and from the organization outwards – to customers and suppliers)

4 Cloud computing and software procurement

Sign with the vendor a contract that requires compliance with accepted standards for software and information defense, such as the supply chain methodology of the cyber directorate. In particular, when uploading to the cloud, the division of Cyber Defense responsibility between the cloud provider and the organization must be ensured.

5 Information Defense

Define defense mechanisms for how information is taken out of the organization

6 Defense of Computers and Peripherals

Set the required level of defense for the computers. This level includes changing default passwords, removing unnecessary software, hardening external interfaces, and removing non-essential user accounts.

7 Human Resources

Instruct employees when they are hired, raise their awareness and have them sign a non-disclosure of information from the organization after termination of employment. Define policies for the use of private computing equipment and its connection to the organization, and formulate work practices on the network and computers. Define policies for computing and cyber defense personnel (while examining how they are employed as internal or external employees), including awareness and control over their activities

8 Documentation and Monitoring

For future investigation/ debriefing, monitor and document on logs unusual actions that the organization wants to know if they have occurred, and which indicate a cyber threat

9 Network Security

Make sure that access to the network is under the control of the organization (vendors and employees cannot remotely connect to the network when and how they choose) and that the network is prepared for denial of service attacks. In particular, the exposure area should be reduced and it should be examined whether the organization is exposed to the world through unnecessary and/or unsafe interfaces.

10 Business Continuity

Ensure recovery capability in cases of a website crash, information deletion or file locking. In particular, the existence of an effective backup must be ensured. An initiated restore should be performed periodically and the frequency and type of backup required should be defined

After examining the status of the implementation of the controls, it must be decided what is the required response to the risks arising from the gaps in the implementation of these controls. These risks are often divided into breaches of data confidentiality, business continuity and information integrity. These risks can have many consequences, such as damaging the reputation of the business; inability to receive customers and provide them with service; exposure to claims due to violation of legislation and/or regulation; or leaked information on customers, who may eventually sue the organization. These risks must be examined against the Defense objectives defined in Stage 1.

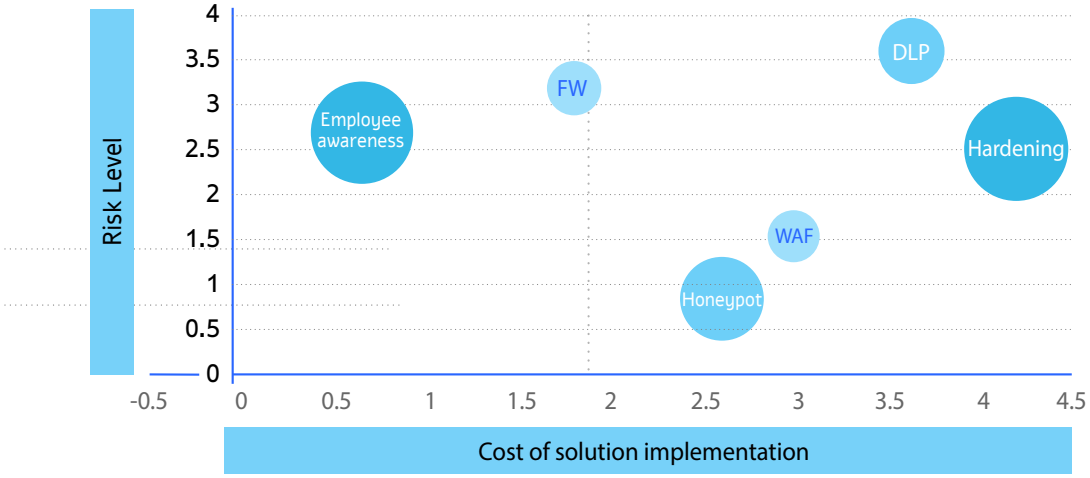
Stage 4: Building a work plan

Once the organization has defined the risks to its defense objectives, an annual plan must be drawn up to reduce and/or transfer them, in accordance with the decision in stage 3 above. This plan may include implementing processes and procuring solutions such as: Periodic inspection of the backups in the company, protection of laptops, installation of protection software for end stations, and training of employees in the organization.

In building the work plan for closing the control gaps, the following considerations must be taken into account:

- **Control effectiveness** – its contribution to reducing the risk to the organization.
- **Cost of realizing the solution** – represented below by the "cost of solution" axis (duration of implementation, complexity of implementation, manpower and equipment required).
- **Application speed** – represented below by the size of the circle.

Example of parameter weighting for determining the priority of the work plan for a category A organization.



The risk level of the asset – the y-axis in the example below.
The cost of implementing the solution – the x-axis in the example below.
Speed of application of the solution – expressed by the size of the circle in the example below.

The following is an auxiliary table for filling out data:

Defense targets mapped in the organization	Such as: Website, customer database, end stations, email server, backup server, etc.			
The control family	Exists/Does not exist	Control effectiveness	Realization cost	Data weighting / prioritization
Management Responsibility				
Malicious code prevention				
Encryption				
Cloud computing and software procurement				
Information Protection				
Computer Defense				
Human Resources				
Documentation and Monitoring				
Network Security				
Business Continuity				

The proposed work plan will be approved by the organization's director.

Stage 5: Continuous auditing and control

The pace of implementation of the work plan and its relevance should be periodically examined. The purpose of this stage is to check if there are any new information assets, what controls have been implemented so far and what resources and inputs are required from the organization's management on the subject.

The audit may be conducted in parallel with a periodic review (for example, annual or biennial) or with reference to cyber incidents that have occurred in recent years in small businesses in Israel and abroad. The audit will help management focus its efforts and prioritize resources according to the more relevant risks for the organization.

A Category A organization has finished reading this document.

4.2 Implementing the Doctrine of Defense for a Category B Organization

Stage 0: Corporate governance and strategy for corporate risk management

Before identifying the threats and responses in the organization, the corporate governance that supports the process (sometimes called ISMS – Information Security Management System) must be examined: Its purpose, definition of hierarchy, functionaries, Defense routines and control procedures performed. The goal is to map the cyber risks and the response given to them, while presenting continuous improvement.

As part of the definition of corporate governance, the organization must address the following issues:

- Who is the party/body/person that performs the risk assessment within the organization? What is his training and experience in the field? What are the resources available to him? Who is the officer to whom he reports within the organization?
- Is there a mapping of sensitive processes in the organization as part of the Business Impact Analysis (BIA), which can be used for risk assessment? How does risk assessment fit in with the organization's goals?
- Which method will be used to identify new risks and what tools are available to the organization to identify them effectively?
- What is the frequency of risk assessment? Will the risk assessment be performed in the light of attack scenarios and attribution threat or in accordance with the organization's overall risk management methodology (ERM)?
- Who is the authorized party to decide on taking a risk? Who is authorized to approve the risk reduction activity? Who is authorized to update the risk to a lower value, in light of the implementation of Defense controls and remedial/compensatory activity?
- Is there a steering committee on Information and Cyber Defense? And if so, who are its members? Is there a steering committee on the issue of business continuity? And if so, who are its members?

Stage 1: Demarcation of activity and risk assessment survey

Demarcating the defense objectives is an initial and necessary step in order to understand the environment in which the organization operates and to define the boundaries of the sector and the areas of responsibility.

At this stage, the organization will define, among other things, the following topics:

- **The boundaries of the demarcation between the Chief Information Security Officer (CISO) and other functionaries in the organization** – the division of authority and responsibilities with internal stakeholders, such as the Security Officer, Operations Manager, Information Systems Manager, Risk Manager, Legal Adviser and CEO. If the organization needs cyber and/or computing services as a service (MSSP), it is important to define the interaction and division of responsibilities between the parties.
- **In-depth knowledge of the organization's strategy** (including vision, objectives, characteristics of the business market and competitors), and how the issue of information Defense and cyber fits into it.
- **What is the demarcation of the risk survey** – Does the survey include aspects such as security cameras, air conditioning system, production line and operating environments, private computing devices of employees, supply chain and branches outside the country.

At the end of this stage, the organization will have a document describing its business environment, characteristics and demarcation of the survey activity.

This stage may have implications for business continuity documents, an organizational IR plan, supplier engagement contracts, a BIA document, merger and acquisition (M&A) processes, and more.

Stage 2 : Risk Assessment

This stage consists of three sub-stages: Risk Identification › Risk Analysis › Risk Assessment.

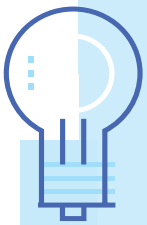
There are many risk assessment methods, including FAIR, OCTAVE and ISO 27005. Each has unique characteristics and benefits. This document presents a method that combines many advantages of the known methods, and adds to this knowledge from practical experience gained in the field, while adapting to the Israeli economy.

2.1 | Risk Identification – This activity consists of the following two sub-steps:

- **Mapping defense targets** – understanding the potential targets that the organization is required to protect in cyber aspects. This mapping may include a list of assets such as applications, networks or operating systems. The mapping can also include a list of important business processes, associating the digital assets that serve those processes (such as a payroll process, stock exchange reporting or credit card clearing). It is advisable to give priority to mapping business processes over mapping the defense objectives, while analyzing the various interactions.
- **Assignment of risks and/or threats and vulnerabilities** – After mapping the defense objectives, the cyber threats relevant to the processes and assets identified must be examined. For example, what are the possible courses of action through which an attacker can realize the threat – for example, disrupting the production process or gaining access to the organization's sensitive database. In Appendix B of this document you will find a list of common threats and vulnerabilities.

For the purpose of performing a comprehensive mapping of IT assets, it is recommended to obtain a list of assets from the information systems division in the organization. It is also important to obtain from the Procurement Department a list of suppliers of products and services, which may detect systems that are provided as a service and are sometimes not managed by the organization's central computing body (Shadow IT). For the purpose of mapping OT (Operations Technology) assets, it is recommended to meet with the Operations Officer and the Security Officer (especially in industrial organizations).

An organization that has formulated a business continuity plan will be able to use it for the benefit of mapping material business processes (using BIA).



Target mapping resolution

Mapping defense targets is a process that requires time and resources. In order to carry out the process effectively one must pay attention to the resolution of the mapping.

For instance: On the one hand, it is clear that it is not necessary to list all the servers and all the end stations, and on the other hand – a gross generalization of all the servers as one piece may result in disproportionate defense costs (over-investment or lack thereof versus the real risk).

Attention: Sensitive information of the organization is sometimes found at the vendors' premises or stored in the cloud. Also, sometimes sensitive information is stored within a file rather than within a dedicated database or information system. Good mapping also includes such assets. An overview of the core processes of a business is a good way to make sure that the mapping takes into account all the essential assets.

Impact X Likelihood = Risk

Risk Analysis – The purpose of this step is to determine what incidents may occur, based on the information in the organization's possession. There are various methods for assessing the level of risk posed by each possible incident. One of the most common methods is to use a formula:

This formula relies on the ISO 31000 standard, which defines the risk as a product of the intensity of the potential damage with the probability of its realization (what are the damages that will be caused if the incident occurs, and what is the probability of its occurrence).

Calculation of the magnitude of the damage – is usually performed while examining the maximum damage potential as a result of a breach of confidentiality/reliability/data availability (CIA). To calculate the magnitude, it is recommended to use the following table:

Question	1	2	3	4
1. What is the level of damage that will be caused to the organization following **the disclosure of information** from the process/ property? **C** **Confidentiality**	The estimated damage meets one or more of the following criteria: a) Cost of up to USD 1.5 million for the organization. b) Investment of up to two months of human work for the purpose of handling the incident. c) The property is defined as a database managed by an individual under the Privacy Protection (Information Security) Regulations.	The estimated damage meets one or more of the following criteria: a) Cost of between USD 1.5 and 3 million per organization. b) An investment of more than six months of human labor, but less than 5 years for the purpose of handling the incident. c) The property is defined as a database on which the low level of security applies according to the Privacy Protection (Information Security) Regulations.	The estimated damage meets one or more of the following criteria: a) Cost of more than USD 3 million for the organization. b) Investment of more than 5 years of human work for the purpose of handling the incident. c) The asset is defined as a database to which the medium level of security applies in accordance with the Privacy Protection (Information Security) Regulations. d) There is a possible danger to human life.	Significant damage will be caused, which will meet at least one of the following criteria: a) There is a clear and immediate danger to the lives of many people. b) Economic damage estimated at more than USD 30 million. c) The property is defined as a database to which the high level of security applies according to the Privacy Protection (Information Security) Regulations<?>. d) There is a clear danger to public health. e) There is a clear danger to human life.
2. What is the level of damage that will be caused to the organization as a result of **the disruption of the information** (or data) in the process/property? **I** **Integrity**				
3. What is the level of damage that will be caused to the **organization following the shutdown**/ cessation of the process/property for an extended period of time? **A** **Availability**				

The value score for each process/asset is the highest score obtained for the three questions (Impact = MAX 1-4). This score is also called the **magnitude** of the risk (marked with the letter I). It defines the maximum potential damage to the organization as a result of harm to this process/ asset.

Attention:

In the field of Cyber Defense and information security, it is common to examine the damage that can be caused by three categories:

- **Violation of data confidentiality** – for instance, a cyber attack for leaking customer information or a trade secret to the Internet.
- **Impairment of data reliability** – for instance, a cyber attack that changes the data of the company's financial report so that it does not properly represent its situation, or an attack that disrupts the proper functioning of the production line.
- **Violation of data availability** – for example, a cyber attack, which causes the information to be unavailable to the company or its customers. For instance, when a site crashes or files are locked (ransomware).

Tip: Biases are common in assessing property values

The analysis of the value of the assets must be performed in collaboration with the business bodies. Property owners from the business side sometimes feel "overvalued" and believe that their property is the most important in the organization. Adherence to the value questionnaire criteria will neutralize such feelings and help to assess the systems on a uniform and bias-free scale.

Note that impairing data reliability can sometimes have implications for processes in physical space. Therefore, in the risk assessment process it is important to examine the meanings of cyber attack on Operating Systems (OT), Industrial Controllers (ICS), security cameras, control and monitoring systems, or equipment which is often not managed by IT personnel.

Calculation of the degree of probability – may be based on a weighting of several parameters. Among the parameters that can be taken into account:

a. **Incident History** – An overview of cyber incidents that have occurred in recent years, while examining the sector in which the organization operates, its characteristics, its typical systems, etc. The goal is to understand the types of attacks known in the world and the frequency and prevalence of each type of attack. Understanding the trends in the world of cyber attacks will assist at giving weight to recent incidents, thus preparing for the current challenges of the organization/sector.

b. **Cyber intelligence** – Finding intelligence on the web (using internal resources or purchasing an external service) will allow the organization to get a more accurate picture, as well as prepare for a point-by-point defense based on the image seem from the attacker's perspective.

c. **Ease of realization** – The ease of realization of the attack can be affected by many variables, such as the size of the attack surface (including the amount and type of users), the level of defense and physical accessibility to the asset, the amount and type of interfaces, or possible courses of action of the opponent in relation to the critical paths (paths of entry into and exit from the organization).

d. **Motivation for the attack and the type of information** – the size of the database, the type of database, the identity of its owner, the existence of business competitors and other parties often affect the motivation of various stakeholders to attack the organization. For example, systems that include medical and/or financial information are exposed to a different level of threat than systems with a different type of information.

Weighting the motivation, types of information, stakeholders and potential damages can help the organization produce a more accurate risk map, which takes into account the opponent's vision. The following table can be used as a tool to support decision making in the process:

Players	Motivation	Goals	Effect/Influence
Government / emissaries / sponsorship	Espionage	Corruption and disruption of information	Injury to human life/safety
Criminal organizations	Military	Intellectual Property	Loss of income/economic damage
Employee with privileges	Pre-mission intelligence	Leak of sensitive/ confidential information	IP theft
Terrorist bodies	Political	Services	Damage to Reputation
The activists	Financial profit	Image and reputation	Infrastructure destruction
Business competitor	Disabling/interrupting/ sabotaging		Indictment/prosecution
A lone and skilled hacker	Competitive edge		Sanctions and restrictions
Kiddies script	Anarchy/Chaos		Loss of public trust/investors
	Revenge/resentment		Hampering functional continuity
	Tactics/Strategy		The environment
	Social/moral		Perception
	Issuance of a statement		

For the purpose of calculating the probability, the following table can be used. A score ranging from 1 to 4 must be given for each of the parameters/tests. In the parameters built from a number of sub-sections, each section must be given its own score (between 1 and 4) and finally the average of the answers in all sections must be calculated.

Parameter/ Criterion	Auxiliary questions
Incident History (Value ranging from 1 to 4)	Has a cyber incident occurred in the organization and/or at the premises of the organization's suppliers in the last five years?
Cyber threat intelligence (Value ranging from 1 to 4)	Do cyber intelligence findings indicate that information held by the organization is a preferred target for attack?
	Do the findings of cyber intelligence indicate that the organization and/or the organization's suppliers and/or organizations in a similar activity sector in Israel or across the globe constitute a preferred target for the attack?
What is the Attack Surface (Value ranging from 1 to 4)	What is the level of physical security of the process/property?
	What is the update policy and security patch?
	What is the level of up-to-dateness of the process/ property?
	What is the level of privilege compartmentalization in the system?
	Is there remote access to the system?
	What type of information is in the system?
	What is the nature of the process/property interfaces?
	How many interfaces does the system have?
	Who are the human users of the process/property?
	Number of users (human/applicative/computer) in the process/property?

The score given for each parameter must now be placed in the formula below. Attention: Each parameter can be assigned a coefficient at a different magnitude, depending on its importance to the organization (the total amount of the coefficients should be 1). In the example presented here, the attack surface parameter was given the greatest importance (coefficient 0.5), while the incident history parameter is estimated to be less important (with a coefficient of only 0.2).

Likelihood = {0.2 (Incident History Score) + 0.3 (Intelligence Score) + 0.5 (Attack Surface Score)}

Calculation of the level of risk to the asset – how the data is weighted

"Inherent risk" – calculated by weighting the intensity of the potential damage (Impact), which is derived from the value of the defense target, and the degree of probability that a cyber incident will occur in this property or process (Likelihood). The calculation can be done by placing the intensity/ valency values (I) and the probability (P) in the matrix below (the risk increases the higher the number and the color turns from green to red):

ערכיות (I) / סבירות (L)	4	3	2	1
4	16	13	10	7
3	15	12	9	6
2	14	11	8	5
1	13	10	7	4

"Residual risk" – Since organizations implement defense controls, such as managing access, encryption, or monitoring permissions, the level of risk they actually face is less than the root risk level. After weighting the existing controls in practice, the level of risk is represented by the value called "residual risk".

Sometimes the organization can reduce the risk by reducing the potential for damage (Impact) – for example, by creating an effective backup system or purchasing cyber insurance. However, for the most part, the organization reduces the risk by reducing the exposure area and reducing the likelihood of a cyber incident materializing. This is done through the application of controls, technologies, procedures and defense processes.

To calculate the residual risk, the risk level (calculated in the matrix above) should be reduced according to the actual level of implementation of the existing controls. Thus, the residual risk level can be represented using the following formula:

(Impact X Likelihood) – Controls

Here are two examples of how it can be assessed at how many levels the implementation of controls will reduce the risk:

- A test that will show, for instance, that the implementation of all controls will reduce the level of risk by two levels, while the implementation of 50 percent of them will lower it by one level.
- Carrying out a risk reassessment (intensity and reasonableness), assuming the organization implements the controls it has decided to incorporate into the reduction plan.

2.2 | Risk evaluation – After formulating a list of risks and/or threats, ranked according to the priority of treatment, each of them should be assessed in comparison with the level of risk acceptable by the organization.

"Target risk" – when the residual risk level is higher than the risk level accepted by the organization (known as Risk Appetite), a mitigation plan must be elaborated that aims to reduce the residual risk to the desired risk level (unless management has decided on a different risk management strategy, such as its transfer or acceptance).

A review of the professional literature found that there is no accepted method and/or international formula for calculating the risk of the target. Thus, one of the following two alternatives can be used:

- Use the method by which your organization performs risk management (compliance risks, credit risks, operations risks etc.).
- Using guidelines to be defined by the organization, such as defining a maximum risk that the same organization can contain (e.g., a decision not to reach a risk level in excess of 10), elaborating a plan to mitigate the risks found in the heat map above this value, and reducing the high risks.

For the purpose of defining the target risk and appetite risk as a function of the root risk, it is possible to use a tool such as this:

	1	2	3	4
	Damage potential			
Danger of loss of human life	Severe danger to the health of employees or customers	Slight danger to environmental health	Without obvious risk	Human damage
Economic damage estimated at more than USD 30 million	A cost of more than USD 3 million for the organization	Cost of USD 1.5–3 million for the organization	Cost of up to USD 1.5 million for the organization	Economic damage
Danger of closure to the organization as a result of the incident	Investment of more than 5 years of human work for the purpose of handling the incident. The organization will suffer irreparable damage or severe and prolonged impairment of functional continuity	An investment of more than six months of human work, but less than 5 years, for the purpose of handling the incident and returning to routine. Moderate damage to service to customers and stakeholders	Investment of up to two months of human labor for the purpose of handling the incident until returning to routine. Slight damage to service for customers and stakeholders	Operational damage
The organization will lose the trust of its customers and suffer widespread and harsh public criticism	The organization will lose a competitive edge and its position vis-à-vis its competitors and customers	The organization's image will be damaged while managing the incident. Potential for class actions	No significant image damage is expected	Image damage
Severe damage to the environment in an irreparable manner	Serious invasion of privacy of employees or customers of the organization	Moderate damage to customers or suppliers of the organization (supply chain)	Slight damage to the continuity of the service provided to the company's customers	Social/ environmental /external damage

	1	2	3	4
Defining the risk appetite in relation to the most serious risks for a particular organization				
	A leak of the entire medical database, which will cause irreversible damage to the organization's customers	Fear of economic damage as a result of loss of information originating from an internal party – with an emphasis on those with high privileges in the enterprise CRM system	In the case of ransomware that also includes theft of information, the economic damage is estimated at half a million to a million USD.	Violation of information confidentiality
	In the case of damage to the production line (ICS) due to a cyber incident, the expected damage is estimated at tens of millions of USD, with significant damage to functional continuity		In the case of ransomware, it is estimated that a week will be required for recovery from backups. There will be a slight impairment in functional continuity	Impairment of information availability and functional continuity
Cancellation of work orders and contracts with the organization to the point of eminent closure of the organization, due to the disruption of the data in the main database of the organization, which includes the information at the core of the service provided to our customers		in the case of a disruption of the reporting process to the stock exchange and a disruption of the financial statements data, the damage to the organization will include damage to the image and financial cost estimated at several million New Israeli Shekels.	Financial damage amounting to hundreds of thousands of shekels as a result of working with information that is managed in applications that do not allow audit trial, permission management, version management, etc. In the case of information disruption, several months of work will be required to correct and recover the data	Impairment of the reliability of information and data

At this stage, an assessment of the risks analyzed is made and a decision is reached as to how to cope with those risks. The decision must take into account, among other things, the following considerations: The level of criticality of the business process; the topology of the organization; Information systems and service providers or product that are involved in the critical processes; and ability to respond and handle risks.

At this stage, the organization will have a table summarizing the risks identified and rated. This table might look like this:

The name of the risk	Scenario description	Likelihood (score in the range 1-4)	Intensity (score in the range 1-4)	Root risk (weighing power and likelihood)	The quality of existing controls	Residual risk
Loss of competitive advantage as a result of leaking sensitive information	Unauthorized possession of information by an employee of the organization via a mobile memory device or sending it by private/business email					
Loss of revenue as a result of disabling communication between branches	A ransomware incident in the corporate/ organization network					
Legal exposure due to non-compliance with legislation and/or regulation	Uncontrolled release of information by a provider by uploading it to a cloud service					
Loss of income due to inability to clear transactions	Denial of service attack on the company's website					
Reputation damage as a result of an intrusion into the systems of a key organization supplier	Utilizing a remote access interface to the organization through the organization supplier					

At the end of this stage, the organization will have at its disposal a map of rated threats/risks.

Stage 3: Handling the risk

As a general rule, it is impossible to carry out an activity without exposure to risk.

Investment of inputs to mitigate the risk should be made while weighing a number of parameters: Economic cost-benefit test for the organization; duration of implementation; the level of probability of the realization of the risk; legal obligations of the organization by virtue of contracting with suppliers and/or by virtue of law and regulation; moral considerations (e.g. social responsibility); and other parameters decided upon by the organization's management.

At the end of this stage, the organization will categorize each of the risks under one of the four options that are commonly used to address risks worldwide:

a. **Risk acceptance** – In the event that the risk is not high, the organization may decide to carry out the activity without the implementation of dedicated defense controls. It is possible to decide to accept the risk even in the case where the measures required to reduce it exceed the threshold of the resources that the organization is willing to invest in the face of the specific threat. For instance: An organization may decide that access to its computers will be performed without a process of strong identification, because of the cost involved in implementing a strong identification mechanism or due to the attribution of low weight to the risk of information in the system leaking.

b. **Risk reduction** – If the organizational activity must be carried out despite the risks inherent therein, it is possible to examine the implementation of defense controls that reduce the likelihood of a cyber incident materializing. For instance: If the organization has sales stands that clear transactions using credit cards, it is common to apply defense controls to reduce the risk of credit information being leaked from them. These controls may include preventing external devices from connecting, managing privileges on workstations, encrypting sensitive data, and more.

c. **Risk Transfer** – In cases where the activity has to be performed, but the organization is not interested in possessing the required defense resources (knowledge, tools, manpower, etc.), the activity can be transferred to a third party. For instance: If an organization is interested in setting up a website or profile on social networks, but does not have the necessary resources to protect it, the execution may be transferred to a subcontractor who will set up the site/profile and protect it. Another

risk transfer option is to purchase cyber insurance against the relevant risk. However, it should be taken into consideration that many times the law does not remove the responsibility of the organization in the case of a cyber incident, for instance a leak of personal information.

d. **Risk avoidance** – In cases where the level of risk is very high and the likelihood of its realization is high, it is possible to decide to postpone the risk by "resetting the likelihood of its realization". For instance: If the organization's management understands that it does not have the knowledge and tools to protect the database it wants to establish, it may be decided not to hold such a database, or not to store very sensitive information in the first place.

Application of Defense controls

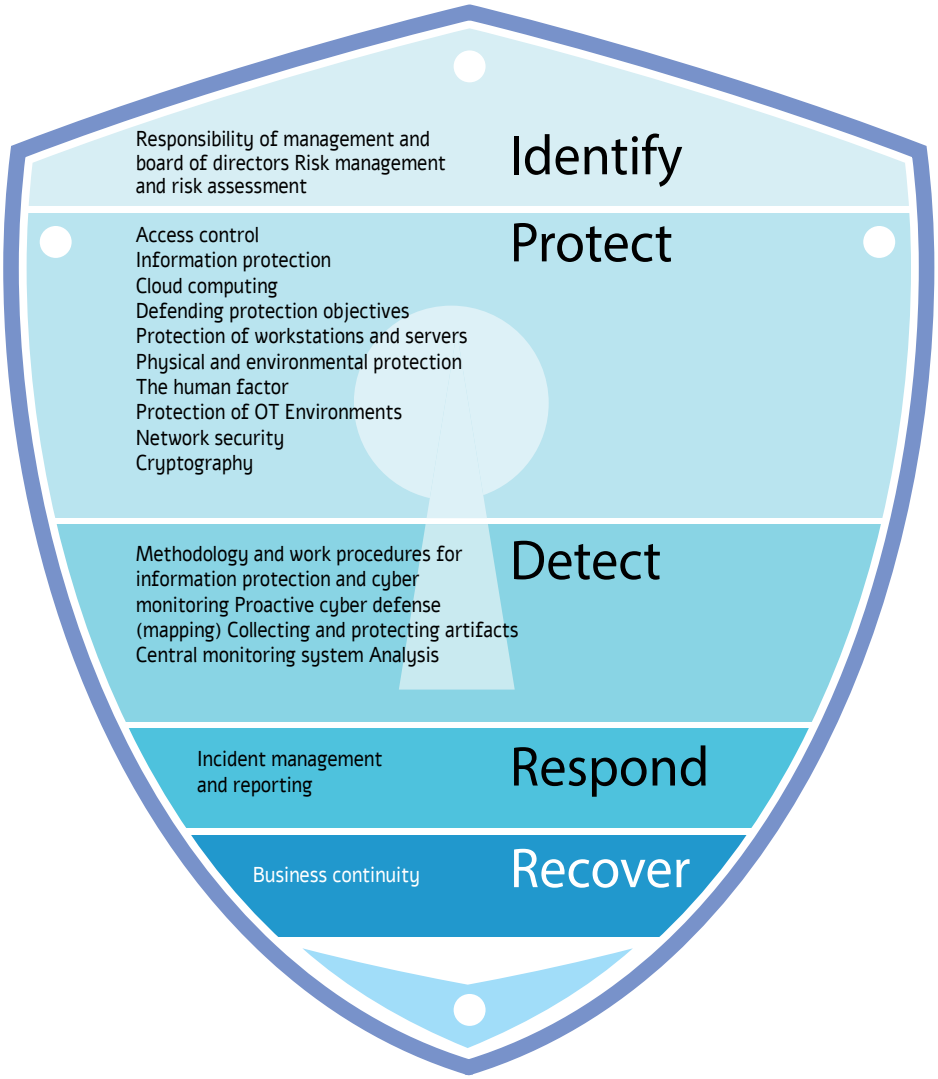
Once the organization has decided on the assets/processes in which risk reduction activities are to be carried out, defense controls must be created for them. The controls consist of processes, products and people, who perform various activities aimed at reducing the cyber risks to the organization, such as: User management, encryption, monitoring, backups and more. The level of Defense for each asset/process is directly affected by its residual risk level.

The Cyber Defense routine consists of the design, implementation and assimilation of Defense controls. This chapter forms the basis for this routine, and for the benefit of its implementation, Appendix C in this document and the database of controls of the Defense Doctrine that appears on the website of the Israel National Cyber Directorate must be used.

It is customary to present the various controls within the framework of conceptualization that reflects the connections between them (Framework). Dedicated controls were written at the Israel National Cyber Directorate that correspond to the latest threat outline, which are incorporated into a framework similar to that of the NIST Cyber Security Framework. These controls make it possible to bring the extensive professional knowledge and experience accumulated in the local cyber directorate, and at the same time enable organizations in the economy to operate in accordance with accepted work frameworks around the world.

Defense Doctrine controls include unique characteristics, including the construction of the "depth of application of the implementation", the presentation of emphases for the optimal implementation of a specific control, as well as the emphasis and evidence required to build a professional infrastructure for certification for this method.

Defense Doctrine Control Framework



To decide which controls are relevant to a business/asset process in which the level of risk must be reduced, go through the list of defense controls in Appendix C. Perform a "Gap Analysis" process, defining the depth of application required in each relevant control. At the end of this process, the organization will receive a list of required gaps and controls – depending on the depth of the relevant application.

Because different controls address different risks and processes, organizations sometimes choose to implement the review of controls "continuously" and actually use them as a checklist. The main disadvantage of this method lies in the fact that the organization examines the controls in a "compliant" and oriented towards compliance with regulation/standard, and not in a risk-based vision (Risk based Vs Control based).

Since not all controls are implemented in the organization in the same way, and not all controls are required for every process/asset, make sure that for defense targets which are material for the organization an individual test is performed. Experience shows that although controls are usually implemented in organizations across the board, there are quite a few cases where the control has not been implemented in a specific process/system.

Since not all controls are required in each asset, use the value level defined for each asset in stage 3 to target the gap list. This list will be the basis for building the organization's work plan (Step 4).

At the end of this step, the organization will hold a list that may look like this, for example:

Control	The whole organization	The CRM system	Supplier Payment System
Multifactor authentication must be implemented for logging accounts with over privileges over the network, depending on the depth of application X	Partially present	Present	Must be realized/ materialized
Security measures must be defined and implemented in order to detect and warn of unauthorized changes in configuration settings, depending on the depth of application X	There is an orderly process in the organization	The system is in the cloud and we have no direct control over the implementation of this requirement, but requirements can be placed on the supplier	Present
Contractual and legal tools should be used when purchasing an information system or service provider, depending on the depth of implementation X	There is no orderly process of obtaining signatures from suppliers in the organization	The supplier signed a statement	This is a supplier from abroad whose signature we cannot obtain. We will examine the requirements in the face of the generic agreement with the supplier

Stage 4: Building a work plan

After mapping the defense objectives and examining the controls that need to be implemented in the organization for the purpose of reducing residual risk (depending on the depth of each selected application), a process of prioritization should be carried out and a work plan for implementation should be defined.

In order to optimize the order of actions and maximize the benefit derived from the resources allocated in the work plan, it is worth considering the opponent's vision. It is worth noting that much of the information required to complete this step should be derived from step 2 – "calculating the degree of probability".

The classification of attackers and attacks may be streamlined according to the following division:

- Source of attack: Internal body in the organization, external partner/ third party of the organization, a body/party which is external to the organization.
- Reason for attack/incident: Accidentally or intentionally

This division will present the organization with a matrix that will focus the organization on threats that need more attention, for instance: An internal employee who tries to maliciously extract sensitive information from the organization; a third-party service provider who inadvertently causes damage as a result of his low level of defense; or an external attack aimed at harming the organization or otherwise achieving benefits.

This approach may target the organization and help classify risk areas where no resources have been invested in handling them.

However, an analysis of many incidents showed that in the vast majority of cyber attacks one of the following channels was used:

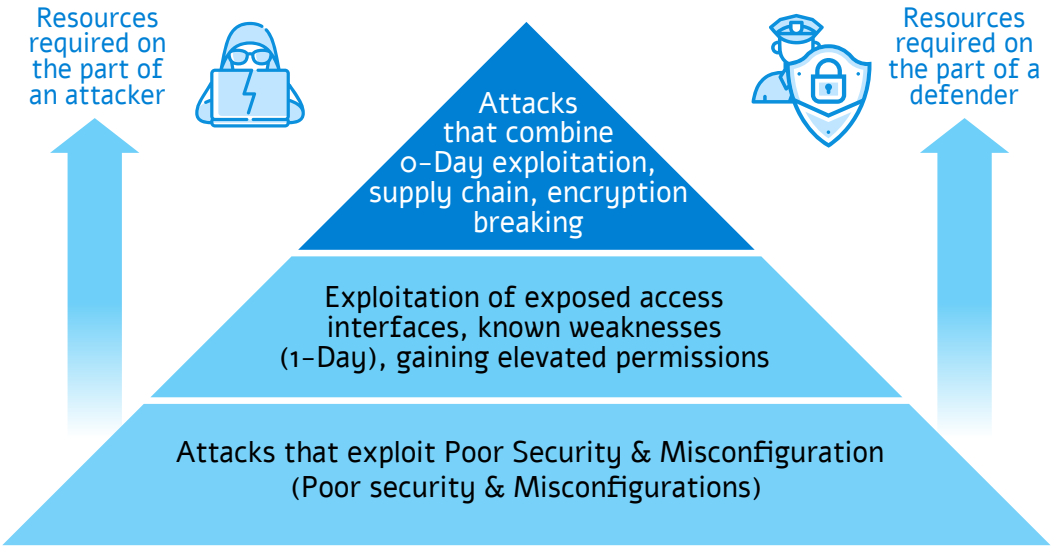
1. **Abuse of external interfaces** such as RDP, SSH or FTP.
2. **Penetration of malware by sending an e-mail** with a malicious file or a link to an infected website.

3. Surfing infected websites that download malware to the end station.

An attack that is not carried out directly via the Internet requires the attacker a lot of resources and the activation of additional means, such as the use of social engineering, utilization of the supply chain, carrying out burial operations or achieving physical accessibility. All of these make the attack more complex and expensive.

Looking at this perspective directs the organization to give higher priority to projects that make it difficult for the attacker to gain access to and grasp the organization's network. Such projects include, but are not limited to, protecting interfaces (e.g., implementing MFA), protecting the enterprise mail server (e.g., using mail relay, sandbox), and hardening interfaces to minimize the use of dangerous protocols.

The implementation of hardening processes and Defense measures for these paths may provide a solution to the two lower layers in the pyramid below:



It should be taken into consideration that different organizations have different cyber risks, which stem from the unique nature and characteristics of the organization. Thus, for example, an organization whose main source of income is its trading site may prefer to invest in site Defense measures (such as Anti ddos or WAF) before turning to protecting the corporate email boxes.

Ability to respond after an attack materializes, such as a leaked code or documents, or a hijacked account

However, it has been found that for most organizations in the world, defending the penetration channels from the Internet in the various interfaces is the minimum basis required to deal with most types of attacks.

Continuous improvement in the level of resilience of an organization in the face of the threat of attribution it faces may be reflected in the adoption and assimilation of higher-level controls (such as Level 3 and 4 controls). The improvement will also be reflected in the deepening of the effectiveness of the controls ("depth of implementation of the control").

Formulation and adoption of an advanced perception for dealing with advanced threats

An organization that needs to address more advanced threats, which are most often attributed to advanced attack groups or state attackers, is required to carry out planning based on a more complex defense perception.

Advanced defense perception includes addressing aspects such as the organization's ability to develop deterrence in cyberspace, the organization's policy regarding threat hunting, proactive intelligence, bug bounty programs, and the variability of the defense topology and processes performed in the organization. This approach requires organizational maturity and dialog with management regarding "organizational perception" for progressively dealing with cyber threats. For example, the use of alternative mechanisms and redundancies of technological infrastructure may allow an organization whose website has failed to continue to provide the service/information continuously, without interrupting business activity.

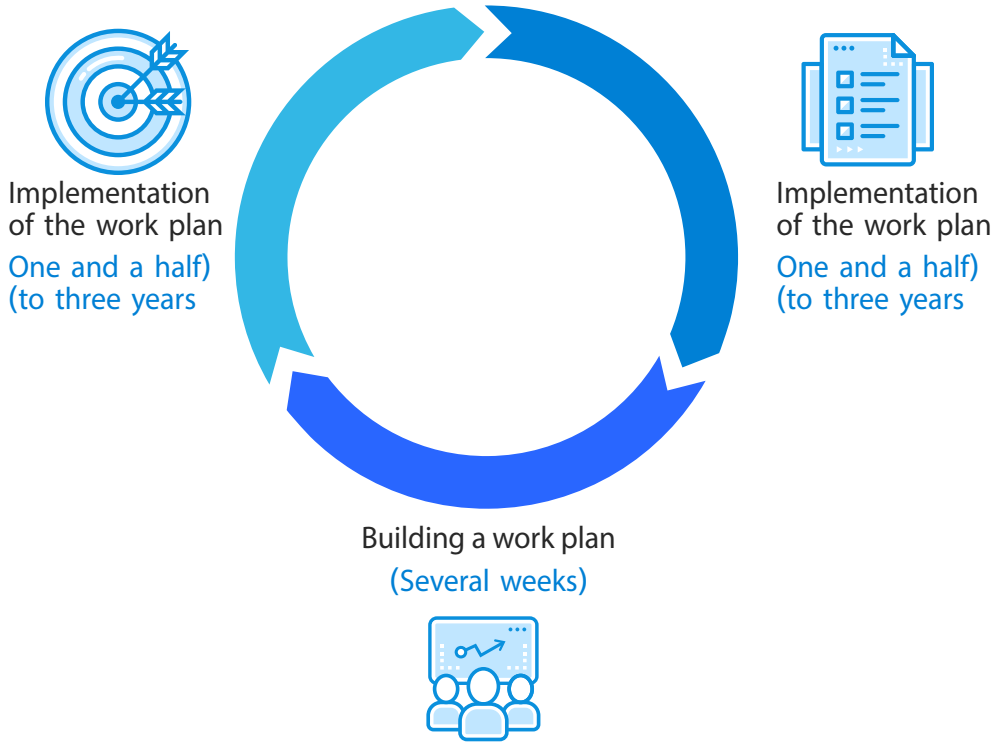
Examples of components in the development of an organizational Defense concept appear in Appendix G in this document.

Step 5 : Continuous auditing and monitoring

Risk management is a process that consists of a number of defined work stages, which the organization performs cyclically over the years. The purpose of the periodic table is to periodically update the required risk map and responses. This update is important, among other things, due to the implementation of Defense controls as well as due to the changes in the internal and external space of the organization.

In addition, organizations have been working to raise the level of cyber resilience over the years through the adoption of "continuous improvement" processes.

Since conducting a comprehensive risk survey in an organization can take a long time, and the implementation of the required steps following it takes a very long time, in many organizations the process looks like this:



For a number of months, an organizational risk assessment process is carried out, after which the organization's management is presented with a map of the risks and measures necessary to reduce them (the work plan). These measures form the basis for the budget planning and the multi-year work plan of the Cyber Defense party within the organization. This plan may include, among other things, the need to initiate procurement processes, assimilate Defense technologies and assimilate procedures in the organization.

This process is not unique to cyber risk management and is also accepted in many other areas where the organization manages its risks (such as compliance risks or operational risks).

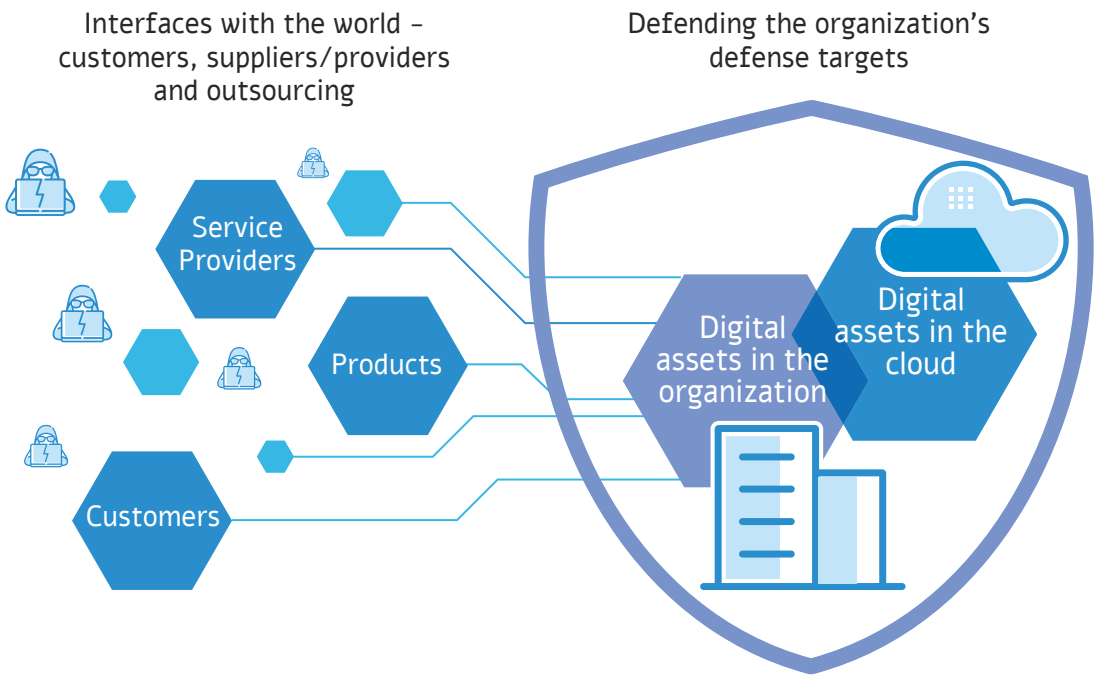
As the pace of change is a critical factor in the digital world, and in particular in the field of Cyber Defense and attack, organizations need to develop the ability to conduct auditing and monitoring flexibly and quickly. This is so that at any given time they can answer the question of **how protected the organization is from cyber threats and what are the immediate steps to be taken in order to minimize these risks?**

Along with budget planning, recruitment and training of employees, and long-term processes that are derived from a horizontal risk survey, an organization is required to simultaneously develop an independent ability to conduct continuous auditing and monitoring. This capability is called "Continuous Control Monitoring" – hereinafter CCM

In order to develop the CCM capacity and its effective implementation, the organization must formulate a concept that will include, among other things, the following aspects:

1. Analysis of how the organization is protected against attacks that originate in the supply chain (Supply chain risk management)
2. Analysis of how the organization is protected against attacks originating from digital assets over which there is no operational or technological control (Digital risk Defense & XaaS)
3. An analysis of how the organization is protected from attacks that originate in its exposure surface, as it appears in terms of intentions and capabilities in the eyes of the opponent. This is mainly reflected in the attack surface management and their vulnerability scanning and Breach Attack Simulator.
4. 24/7 monitoring of infrastructure and systems, whether independently or through outsourcing services.

A holistic view of the cyber risks in the organization



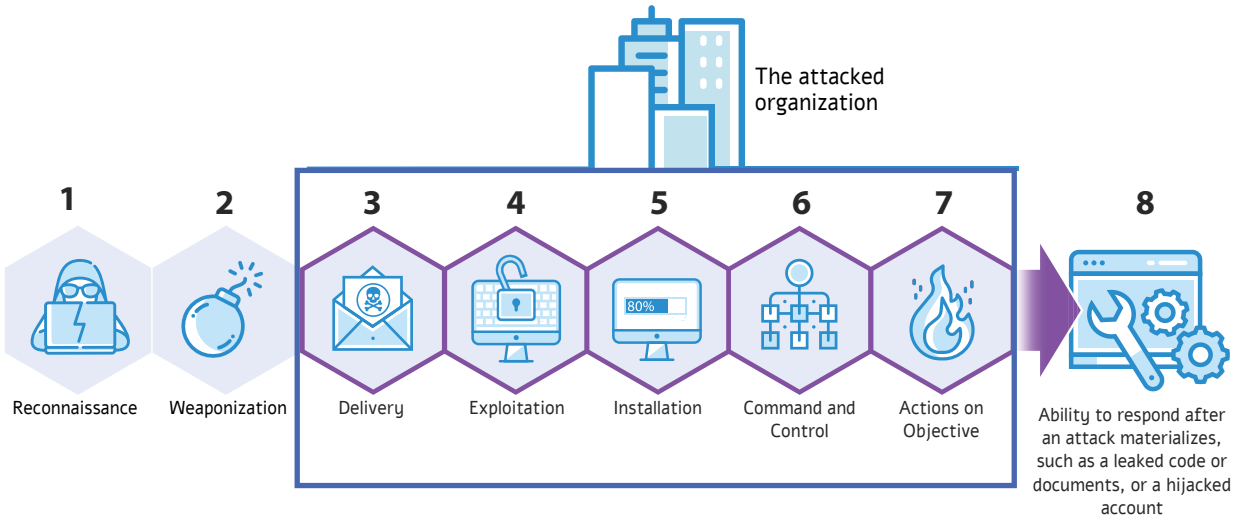
In the past, most of the defense efforts were based on seeing the organization as a closed and demarcated organic unit. Accelerating the use of the cloud, along with increasing dependence on service providers and products, has blurred the boundaries of the organization. Many digital assets that the organization uses, such as social networks, storage services, systems such as CRM and ERP and even mail services are now provided in a "software as a service" configuration (SaaS). This reality requires the organization to holistically examine its internal and external cyber risks, as well as its ability to monitor, respond and recover.

This information is usually managed by a number of tools and services in the organization, including:

- Cyber Risk Management System (VRM – Vendor Risk Management)
- System for collecting cyber intelligence (CTI) and managing the Defense of digital assets such as user accounts on social networks (DRP – Digital Risk Defense)
- A system for mapping the organization's exposure surface (ASM – Attack Surface Management)
- System for examining attack simulations (Breach Attack Simulator – BAS)

Effective implementation of this plan will create for the organization a mirror image that will reflect its level of resilience even from the point of view of the attacker. This image will allow management to show the level of maturity and readiness of the organization in the various content worlds, while prioritizing threats and vulnerabilities.

Post Attack (Code&file sharing, Defacement, Stolen sensitive data, Brand spoofing)



Description of the attack process according to the Cyber Kill Chain method

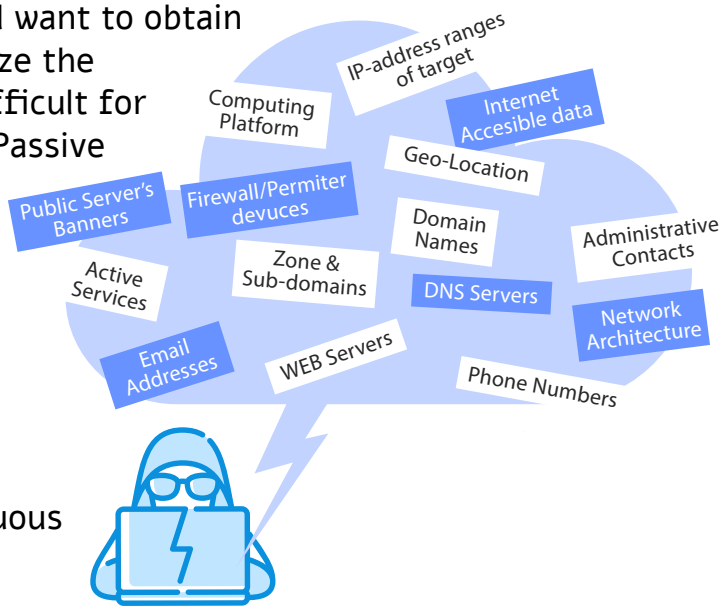
While the defensive side works to reduce the attack surface in all channels and implements defense controls such as encryption, strong identification or hardening of stations, the attacking side can be satisfied with locating one successful intrusion path.

Due to the built-in asymmetry between the defensive side and the attacker a task prioritization mechanism must be created. Tightening all workstations all the time, updating all relevant security patches and raising awareness among all employees and vendors will require multiple resources.

The efficient utilization of the organization's resources requires the ability to produce in real time an up-to-date snapshot of the opponent's opportunity map to execute the attack. The situational picture should be graded, with the aim of achieving the maximum value allowed by the resources allocated for Defense. This rating may be based on parameters such as:

- **In the human axis - who have the highest privileges in the organization? Who are the parties** that have a high media exposure profile?
- **In the technological axis** - what systems are "extroverted" vis-à-vis the Internet? What are the technologies that the organization uses and that any party in the economy may know about?
- **In the process axis** - which projects received broad media coverage? What are the processes that have the greatest impact on the public consciousness or on the business activities of the organization?

Analyzing the information about people, processes and systems in the organization, which the opponent will want to obtain for attack planning, may help prioritize the defense efforts and make it more difficult for the attacker in the collection stage (Passive & Active recon)



Common information that an attacker might be looking for in the Recon stage, prior to the attack

In Appendix D, you will find recommended tools and methods for implementing the principle of continuous control.

APPENDICES

Appendix A – Category A Organization Defense Controls – Emphasis for Computers

Family	Section	The control	Complementary explanation
Management Responsibility	Corporate governance	The organization's approach to managing information security and Cyber Defense, and how it is implemented, should be periodically examined.	The security controls implemented in the organization, information security policies, and the Defense of business processes critical to the organization should be examined.
Malicious code prevention	Detection and prevention of malicious code at end stations and servers in the organization	Appropriate tools should be implemented to detect and prevent malicious code on endpoints and servers in the organization. These tools will be activated in an active Defense format and periodic scans will be performed.	Since some malwares may infiltrate through security mechanisms, it should be ensured that malicious code handling controls are implemented at workstation level as well.
Malicious code prevention	Automatic updates	Automatic updating of all systems to detect and prevent malicious code in the organization must be enabled.	The organization will run an automatic update from a central server managed by the organization or by a recognized service provider. These updates will ensure that the Defense tools are constantly updated.
Encryption	Criteria for encryption	Uses that require encryption must be defined, and the type of encryption required – in accordance with laws, guidelines, procedures, regulations and business obligations.	The organization will define the information and systems to be encrypted, and will document the configuration of the information encryption. The requirements will be derived from the requirements that apply to the organization or from the requirements for maintaining the information.
Protection of workstations and servers	Hardening Policy	Hardening policies for workstations and servers must be defined, documented and implemented, which provides a solution to the organization's information security requirements.	The organization will define hardening requirements for systems in the organization, with an emphasis on the basic requirements, the frequency of updates and the level of classification. It must then document the requirements in a super-framework, which will serve as a basis for writing the hardening procedures.

Family	Section	The control	Complementary explanation
Protection of workstations and servers	Hardening application	The system should be configured to provide the required minimum functionality, while blocking unnecessary functions, ports, and protocols.	The organization will define hardening procedures for each type of system and server based on accepted practices, so that they include at least the following functionalities: 1. Reducing the attack area ofthe system by blocking unnecessary ports. 2. Shutdown of unnecessary services. 3. Removing Guest User accounts. 4. Preference for the use of secure protocols in communication between servers. 5. Receive updates in an orderly fashion. 6. Blocking sensitive functions of the system. 7. Sending logs on system incidents to server monitoring. 8. Blocking the installation of software by unauthorized users.
Public cloud computing	Shared responsibility	The division of responsibility for service security between the service provider and the organization must be understood, and the Defense controls applied accordingly.	When using public cloud services there is a division of responsibility for Cyber Defense between the issues that are the responsibility of the provider and the issues that remain the responsibility of the customer. This division of responsibilities depends on the nature of the service and the implementation model. The organization must understand the issues under its responsibility and implement the implications of that responsibility.
Public cloud computing	Sensitive information sharing	It must be ensured that data that the organization's regulations and obligations prohibit their transmission are not transmitted to the cloud services.	There are data that the organization must not transfer to storage or processing in public cloud services, due to considerations of regulation or commitment to third parties. Before transferring data to the cloud make sure that they do not fall into this category.

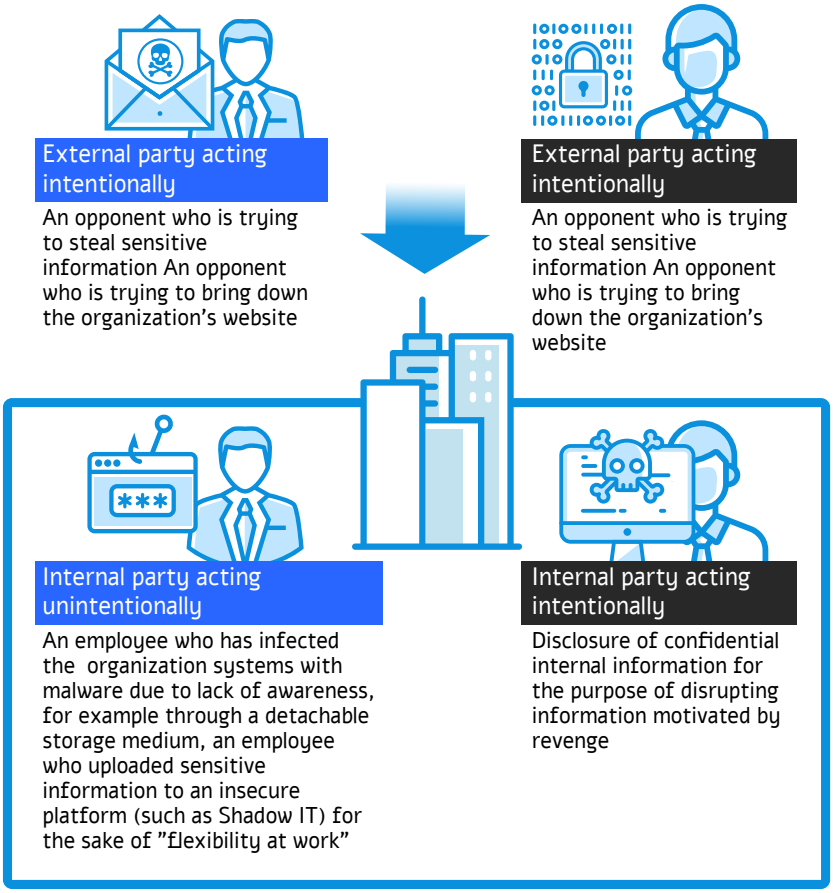
Family	Section	The control	Complementary explanation
Information Protection	Protecting information stored in shared resources	Unauthorized or unintentional transmission of information through shared system resources should be avoided.	The organization must prevent and handle the transfer of unauthorized information through shared folders, e-mail, disconnected media, etc.
Network Security	Session management - at the network level	The organization shall use technological means to protect its services from Denial of Service (DOS) attacks	Protection against various types of denial of service attacks should be made available, such as loading computing resources until they crash, loading communication bandwidth, or loading a website until it crashes.
Network security	Session reliability	Make sure that the Domain Name Service (DNS) is provided by a trusted server (both inter and extra organizational)	The organization will allow the receipt of a Domain Name Service (DNS) only from a secure internal server. This is in order to prevent incorrect communication routes (intentionally or accidentally) to hostile targets
Network security	Network boundaries	The number of communication channels external to the system must be limited	The organization will reduce and unify communication channels, to ensure good control over the connections to the system.
Network security	Network boundaries	By default, all network traffic should be blocked, and desired traffic should be allowed manually by an exception rule.	The organization will define the network traffic filtering rules in a way that blocks by default any traffic that is not explicitly defined as allowed.
Network security	Network boundaries	Separate network addresses (different subnet) must be used to connect to systems in different security zones.	The organization will define that each subnet will have a separate address range that will be posted to the firewall and routers.
Access control	User Management	User accounts should be set up that support the business functions of the organization.	At the very least, an "administrator" account should be separated from a "user" account. Users who manage the security functions in the system (such as user creation, access and system permission management, or information security system management) must also be configured.
Access control	Permission management	Logical access rights to the system and information must be defined and enforced in accordance with the access control policy.	Access control can be done on an individual (identity-based) or role-based level, and its purpose is to control the access of entities (users or computer processes) to objects (files, records, devices and more).

Family	Section	The control	Complementary explanation
Human resources and employee awareness	Employee Rules of Conduct	Rules of conduct must be defined when working with the information systems in the organization. These rules define the areas of responsibility and the rules of proper use, with an emphasis on sensitive systems.	The organization will define behavioral procedures when working with the information systems, and will distribute them to all employees.
Human resources and employee awareness	Managing permissions when recruiting/ mobility/ going on a long vacation (such as maternity leave or unpaid leave) or leaving the organization	An employee's access permissions when moving from job to job should be reviewed and updated.	An update process must be set up regarding employee mobility, and the permissions changed according to the new position (removal of unnecessary permissions and establishment of the permissions required for the new position). Different forms of employment should be considered, for example providers versus organization employees, or organization employees versus outsourcing.
Security in procurement and development	Security requirements in procurement and development of systems	Supply Chain Security – Service providers should be required to comply with corporate security requirements, regulations, standards and guidelines.	The organization will ensure that service providers meet the organizational compliance requirements as well as the regulatory requirements in the countries in which the organization operates.
Physical and environmental defense	Emergency lighting	Automatic emergency lighting must be installed and maintained, which will be activated in the case of a power outage or malfunction. The system will include emergency exits and evacuation routes at the facility.	
Physical and environmental defense	Fire fighting	In order to maintain the information systems, fire detection and extinguishing systems must be installed and maintained, which are supported by an independent energy source.	

Family	Section	The control	Complementary explanation
Documentation and monitoring	Documentation mechanism	A mechanism that generates control records about incidents in the organization's systems must be activated. At the very least, incidents should be recorded from systems that contain sensitive customer information, from systems that are critical to the organization's functioning, and from core systems (servers, communication components, applications, databases, etc.).	The organization will ensure that infrastructure systems and applicative systems operate an incident logging mechanism, and that the records are maintained for the defined period of time. The control records will contain information such as the type of incident, when it occurred, the source of the incident and the username. In any case, the systems that process sensitive information, which are part of the organization's critical infrastructure, or those that manage the organization's core processes should be monitored.
Documentation and monitoring	Documentation mechanism	The registration mechanisms will include, at the very least, information about the nature of the action performed, time signature, source and destination of the action, user identifier, process identifier, failure/ success, mixed file name.	
Incident management and reporting	Handling cyber incidents and information security	Channels of communication between employees and supervisors must be set up for the purpose of reporting suspected security incidents.	The organization will apply procedures that will define cyber incidents that require reporting and determine how to report them.
Business continuity	Resource availability	User-level backups, system and system documentation must be performed, and backup defenses must be ensured.	The organization will back up all the critical information in the information systems that support the business processes, and will ensure the availability, integrity and confidentiality of the backups.

Appendix B – List of Example Threats and Vulnerabilities

All cyber incidents can be classified according to the source of the attack (internal party, provider or external party) and the motive for the attack (intentional or accidental).
The following are examples of different incidents, classified according to this division:



A party involved in the cyber incident versus the motive for the incident

Thus, for example, a file with sensitive information may be leaked out accidentally or intentionally, by an employee of the organization and/or by a provider and/or by an attacker.

Calculating cyber **risk** requires weighting **the vulnerabilities and threats** in the organization. Example of vulnerabilities: Lack of an authorization management mechanism, lack of a mechanism for automatically locking the computer after a period of inactivity, or a weak identification mechanism. A threat exists when there is a party that could exploit the vulnerability in the organization. For example, an internal employee who exploits his elevated privileges, an attacker who exploits the weak password reset mechanism, or a provider who exploits his access to sensitive information.

When calculating the risk, the degree of motivation and the probability of a threat materializing must be examined, taking into account both its degree of prevalence and the degree of its ability to be carried out (by exploiting one or more vulnerabilities).

The threat cause	Manner of realization/ implementation	Potential vulnerability	Scenarios
Remote attacker	Remote listening	Internal IP Phone	Remote activation of the microphone in an IP phone
Remote attacker	Penetration from the Internet directly into the organization's network	Email	Attaching an infected file to the message
Remote attacker	Penetration from the Internet directly into the organization's network	Email	Attaching a link as part of a message to an infected server
Remote attacker	Penetration from the Internet directly into the organization's network	Email	Embedding hostile code in an organization through a message
Remote attacker	Penetration from the Internet directly into the organization's network	Communication gateways	Vulnerability exploitation (CVE)
Remote attacker	Penetration from the Internet directly into the organization's network	Communication gateways	Using an administrator's account
Remote attacker	Penetration from the Internet directly into the organization's network	Web services	Exploitation of vulnerability
Remote attacker	Penetration from the Internet directly into the organization's network	Web services	Injecting hostile code
Remote attacker	Penetration from the Internet directly into the organization's network	Dissemination through the corporate email server	Exploitation of vulnerability
Remote attacker	Penetration from the Internet directly into the organization's network	Dissemination through the corporate email server	Using an administrator's account
Remote attacker	Penetration from the Internet directly into the organization's network	Infecting a station from which the user surfs	Infecting the computer by surfing an infected server
Employees	Malice	Disgruntled employee	Use of his legitimate permissions in the actions authorized for him
Employees	Malice	Disgruntled employee	Use of his legitimate permissions for unauthorized actions or access to information not intended for him

The threat cause	Manner of realization/ implementation	Potential vulnerability	Scenarios
Employees	Malice	Disgruntled employee	Use another employee's account to perform authorized and unauthorized operations
Employees	Malice	Disgruntled employee	Using legitimate management tools on the employee's computer
Employees	Accidentally	Exposure of an internal employee to social engineering	Infecting an employee's computer by Web means (email, surfing)
Employees	Accidentally	Professional negligence	Creating an insecure link between differentiated networks
Employees	Accidentally	Professional negligence	Inadequate or insufficient/incorrect hardening of security and computing means
Employees	Accidentally	Indiscipline	Connecting infected end equipment to a computer
Employees	Accidentally	Indiscipline	Differentiated computer link to the Internet

Organizations that are required to respond to advanced attacks should be prepared to deal with techniques such as:

a. Disabling defense products in the organization, such as antivirus or EDR, in favor of running malwares afterwards. The scenario may be realized,among other means, through:
    1. Rebooting the computer in Safe Mode, which is designed to restore the operating system in the case of a malfunction, since most antivirus programs do not run on it.
    2. Disabling security products by installing kernel-access software and exploiting vulnerabilities of such software.
    3. Disabling security products using malware that contains process killing code.
    4. Avoidance of security products through the use of a virtual machine.
    5. Signing the malware files using legitimate digital certificates.
    6. Using Fileless.

b. Exploiting legitimate software and tools installed on the victim's computer on his own initiative, or installed as part of the operating system tools (Living off the Land) – so using them by the attackers should not arouse suspicion. Dealing with this scenario is not simple for several reasons:

c. The attack is performed using shelf components and software preinstalled on the victim's computer, and without further installation of binary files by the attacker.

    1. Because these tools are often installed by system administrators for legitimate activity, it makes it difficult to block access to them and identify attacks. Moreover, even if the attack is detected, it is difficult to associate it with a particular attack group, because all attack groups use existing tools rather than the tools they have developed themselves.

    2. Among other things, this type of attack can be performed using documents that contain macros, scripts, or using the command interface such as CLI.

It is possible to deal with the exploitation of legitimate software and tools in the ways detailed in the control chapters of the Defense Doctrine method. However, their advanced targeting and implementation in the organization is required. It is also important to define a set of suspicious signs, which will lead to the investigation of a suspected incident. These signs may include adding a user to the Domain admin group, frequently changing file extensions, attempting to query DNS/NTP servers that are not the organization's official servers, or deleting logs.

Extensions about common types of threats can be found in reference sources widely accepted in the field, such as Appendix D in the ISO 27005 standard or in the MITRE[1] project.

The degree of vulnerability can be calculated using tools such as a CVSS calculator[2], which weighs a number of parameters.

Bodies/entities/parties receiving guidance or orientation from the Israel National Cyber Directorate may receive a more up-to-date list of examples of threats and vulnerabilities.

1 https://attack.mitre.org/
2 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Appendix C – Control Bank

The purpose of the control bank is to centralize the Cyber Defense recommendations in the various areas. The control bank will be updated frequently, in accordance with the development of technology and the threats derived therefrom.

The structure of the control bank

The control bank should be built in the form of a table. These are the main columns included in it:

- **Function** – one of the 5 main areas into which Cyber Defense is divided: Identify, Protect, Detect, Respond and Recover. These functions were built in accordance with the NIST CSF framework.
- **Subject and Sub-Subject** – These columns include the control family and chapters included in it. For example, "public cloud defense" family could include secondary issues such as managing cloud changes, working with a hybrid cloud, or functional continuity in cloud work.
- **Control** – the Defense recommendation itself, which must be implemented for the benefit of the risk management process. Controls include recommendations such as appointing a Chief Information Security Officer (CISO), browser defense, or performing monitoring activities.
- **Emphasis in the application of control** – in favor of minimizing the scope of interpretation. The column can also include a breakdown of insights and highlights that will help implement the Defense recommendation appropriately and effectively.
- **Required Evidence** – Documentation that the respondent must present to the applicant to prove that he is indeed implementing the Defense recommendation as required. These measures support audit processes and can help prepare the infrastructure for accreditation and certification.
- **Control Target Level** – For each Defense recommendation a level has been set that moves on an axis of 1-4, with 1 representing basic control while 4 – control to be applied where the potential for damage is more significant. This classification is intended to serve as a decision support tool when considering whether to implement control at a particular Defense target, since not all controls are implemented in the same way in all processes and systems of the organization. In addition, this division helps to produce differentiation in favor of proportionality, so that organizations can start with the implementation of basic controls, and later examine the implementation of more advanced and complex controls.

- **Depth of application/control at level X** – Each control can be applied at different levels of ripeness and depth. Thus, for example, the implementation of a system to prevent information leakage may be carried out only at a basic level (purchase of a product and its basic implementation), but also in a comprehensive way that takes into account the organization's constraints, information classification, adaptation to business processes and more. Level X control moves on an axis that begins with basic level control, which usually indicates a process that exists, but is not managed and executed manually, and ends with the innovative level, which indicates the implementation of control in a managed, documented, automatic, efficient and effective manner.
- **Additional suggested columns** – information about mapping versus additional standards, adding content by the user for performing the gap mapping stage.

How to use the control bank

Working with the control bank involves two main stages:

a. Mapping all the gaps versus the list of different controls (with an emphasis on the "control" column). This mapping helps to understand the issues where the organization is not properly organized and to get a list of gaps (Gap Analysis). The process is obedient/compliance-oriented in nature, and the product is a list of "correct/incorrect/irrelevant/partially implemented".

b. Individual mapping of controls in the face of threats and critical risks in organization-sensitive Defense targets.

Since the implementation of controls is a dynamic process that varies from one Defense objective to another, the level of control for certain Defense objectives must be examined individually. Thus, for example, in certain Defense objectives the ability to monitor, control the supply chain, and the existence of a backup must be examined in detail and in depth. This approach effectively assimilates the transition from a compliance-oriented perspective to a risk-based perspective. Using the control bank as a tool for reducing risks and individual threats constitutes the realization of its purpose in the vision of the organization's management.

Unique characteristics of the control bank in Defense Doctrine

1. **Focus on controls that make the most contribution to Defense** – those whose "cost versus benefit" is the highest.
2. **Depth of implementation of controls** – It is possible to implement controls in various forms, from their implementation in the organization manually and not systematically, to built-in implementation backed by full automation capabilities and up-to-date professional knowledge. For effective and graded implementation, which offers the organization a path to improvement, various options for its implementation are presented alongside each control at a different implementation depth.
3. **Evidence required** – In order to ensure that the controls were properly assimilated into the organization, emphasss and documentation requirements were attached to each of them. This data can also serve as a basis for regulation and/or accreditation/certification in accordance with this method.
4. **Ranking and setting priorities** – For the purpose of building a proportional Defense Doctrine, the controls in this document have been classified on an axis between 1 and 4. Level 1 controls are the most basic, and are required of any organization for each asset, while level 4 controls are only required for a Defense target whose potential for damage is 4.

Appendix D – Tools and methods for implementing continuous control in the organization

Continuous control is essential to the organization, because it presents it with a mirror and serves as its compass. This control allows the Cyber Defense party within the organization to know what the Defense gaps are and what steps are required to improve the situation.

Continuous control can be performed at the compliant level, addressing defined issues and controls (such as compliance status in Defense Doctrine controls), or by measuring risks, threats, readiness for attack scenarios and more.

To build an internal plan for **continuous control** management a number of measurement parameters must first be defined. Mechanisms should then be implemented that will absorb the measurement results and present the current situation alongside the trend in the organization (it is important that these mechanisms be as automated as possible).

Here are some tools and methods that should be implemented in the organization for continuous control:

- **KPI – Key Performance Indicators.** Allow the organization to measure and quantify the level of Defense at a given time, comparing it to the measurement history, thus examining the trend. These metrics may examine, for example:
  - Number of users who clicked on a link as part of a phishing practice.
  - Quantity/percentage of servers and end stations where EDR is installed, where the security updates are up to date, etc.
  - Percentage of sensitive providers for whom a risk survey was conducted.
  - The average length of time from the publication of a critical security update to its installation; The average length of time from the moment of receiving a warning at a given level of severity in SIEM until the beginning/closing of the handling Mean Time To Identify (MTTI)/Mean Time To Detect (MTTD).
  - Percentage of controls not implemented from the standard, number of scenarios/pages to which the organization was prepared.
- **KRI – Key Risk Indicators.** Allow the organization to track the picture that emerges from data collection, and thus perceive the formation of risk. These metrics may examine a trend, but also measure a deviation from a particular set that indicates potential for risk. These metrics can include, for example:
  - The amount of external crawls of the site.
  - The amount of reports that contain sensitive information that is extracted from the system.
  - The amount of information copied to external drives.
  - Number of failed log on attempts.

Rate of changes and measurement

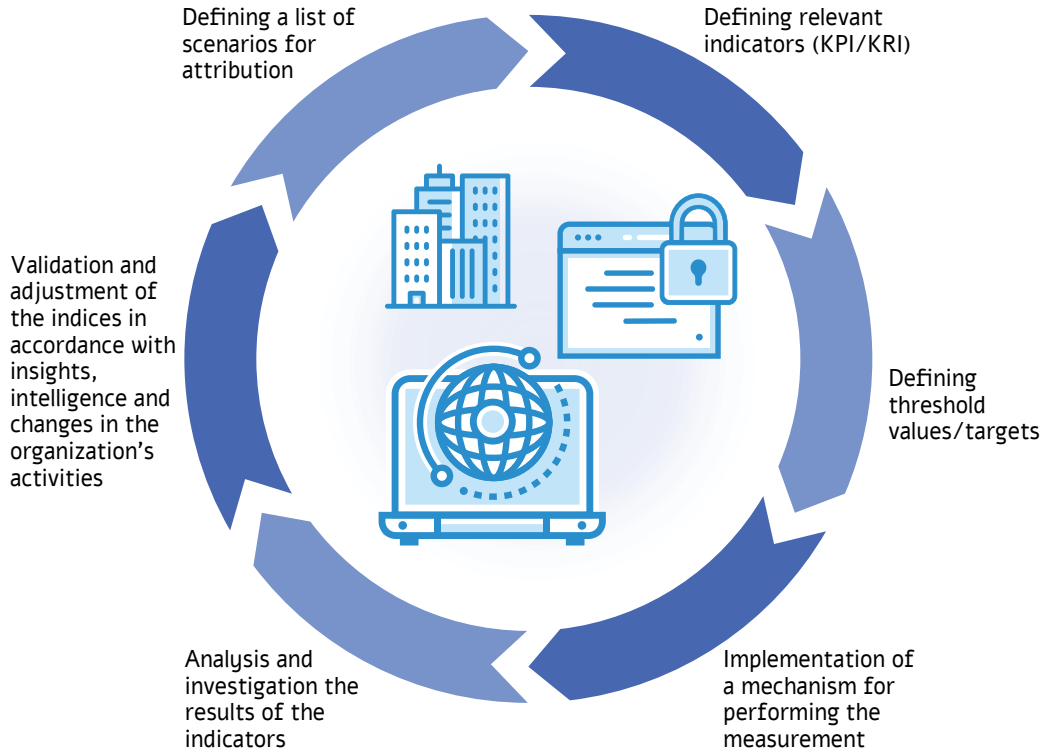
Monitoring metrics such as KPI or KRI requires the organization to sample its status in various parameters at defined time intervals. Many times the process requires manual involvement as well as processing and analysis work, so it takes time. Thus, the metrics may be examined only once a month or quarterly.

In technological worlds the rate of change is rapid, and in order to detect an anomaly some of the metrics must be sampled once a day or even every few hours – and traditional measurement processes do not address this challenge. Parameters that change frequently need a different measurement mechanism, known as "Continuous Control Monitoring" – or in short, CCM.

Assimilating the CCM concept within the organization will allow it to see the situation in real time and in a way that does not require human involvement.

The organization can not "wait" for the next measurement of parameters such as interfaces opened (accidentally or intentionally), critical updates that have not been implemented, a FW constitution defined in a way that endangers the network, or serious security issues in software code. All of these (and more) must be continuously monitored through the implementation of dedicated technology.

The process of assimilating a CCM mechanism in the organization



Emphasis for the implementation of a CCM organizational program

- An organizational hierarchy must be defined, including the division of authority and responsibility in this matter. For instance: How the move fits in with the organization's second line of Defense; Is the chief risk officer in the organization integrated in defining and measuring the metrics; And whether there is a need for Cyber Defense trustees in the various units of the organization.
- The platform on which the measurement process will be conducted must be defined. GRC tools can provide many benefits, although in some cases the process can be managed in other applications as well, such as a word processor.
- The demarcation of the metrics should be examined, while also referring to metrics that "go beyond the boundaries of the organization", for example a measurement of the level of Defense of external providers and subcontractors.
- At the same time as checking the existence of the controls, their effectiveness must be challenged. This test should examine whether a control that has been implemented actually addresses the threats and risks that have been assimilated into the organization. The control challenging may be performed using attack simulation tools, but also through proactive testing of different scenarios. For this purpose, a table of "initiated effective tests" can be used, such as the following:

No.	Control description	Desirable result in case of deviation from approved policy				
		Blocking Activity	Disconnecting from the network	Warning	Investigating/ debriefing and rectifying	Other
1	Activating/sending EICAR test file using a random interface to a cyber asset (such as email, access to Share or surfing the webpage containing the file)	x	x	x	x	
2	Leaking sensitive or confidential information in various interfaces (such as sending to an external email address, uploading to BOX or printing)	x		x	x	Report to user manager

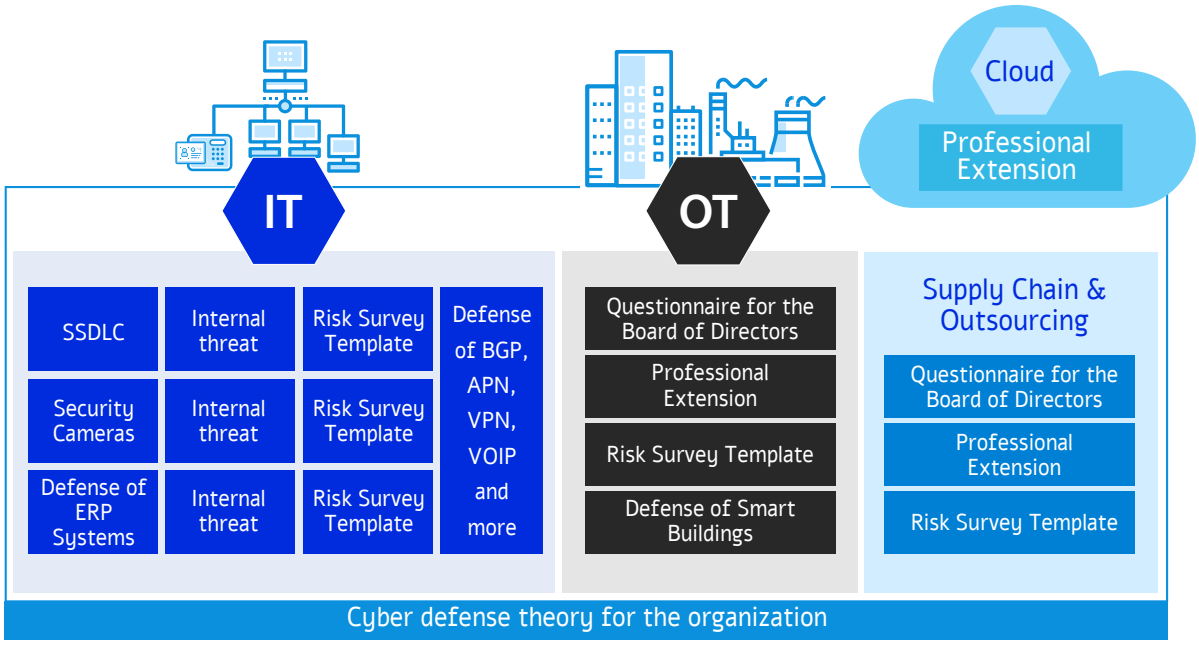
No.	Control description	Desirable result in case of deviation from approved policy				
		Blocking Activity	Disconnecting from the network	Warning	Investigating/ debriefing and rectifying	Other
3	Connecting a DOK device and an external cellular modem to random endpoints	x	x	x	x	
4	Removing/adding a hardware component to an endpoint (for example, memory or hard disk)	x	x	x	x	
5	Performing "Silent" Hostile Network Activity (Example Port Scanning)			x	x	
6	Using a legitimate file upload interface on an internal/external portal to upload a false format-based file (such as an EXE file with a MIME Type value of PDF)	x		x	x	
7	Connecting a computer that does not belong to the organization to a random communication port	x	x	x	x	
8	Examining the number of computers registered in the corporate directory compared to the registry in the Defense system (such as an antivirus management server)				x	
9	Examining the number of users registered in the organizational directory compared to the registration in human resources (or another party within the organization)				x	
10	Activation of an automatic attack tool (such as SQLMap) against an organizational portal (internal/external)	x		x	x	

No.	Control description	Desirable result in case of deviation from approved policy				
		Blocking Activity	Disconnecting from the network	Warning	Investigating/ debriefing and rectifying	Other
11	Examining the hardening configuration of a random endpoint relative to an approved baseline				x	
12	Examining the list of security updates (patches) at a random endpoint relative to an approved baseline				x	
13	Installation/operation of an application that is not approved for use in the organization	x		x	x	
14	Access to a website that violates the organization's permitted policies (such as a file-sharing site)	x		x	x	
15	Attempt to whitewash files that are not allowed on the user profile	x		x	x	
16	Abnormal physical access to classified compounds			x	x	Arrival of a security guard for interrogation + image check
17	Checking the updatedness of the Defense tool at a random endpoint relative to an approved baseline				x	
18	Setting up/modifying/ deleting a user account with elevated privileges			x	x	

No.	Control description	Desirable result in case of deviation from approved policy				
		Blocking Activity	Disconnecting from the network	Warning	Investigating/ debriefing and rectifying	Other
19	Activate two or more stations simultaneously with the same MAC or IP address in different complexes/compounds of the organization	x	x	x	x	
20	Detection of sensitive/ confidential/IOC information at an end station			x	x	
21	Obtaining accessibility from one network to another, even though official policy prohibits direct communication			x	x	
22	Operation of multiple SESSIONS from a single IP address in conjunction with a single server	X		X	X	
23	Operation of multiple SESSIONS from a single IP address in conjunction with multiple servers	X		X	X	
24	Multi-bandwidth consumption from a single IP address or multiple addresses			X	X	
25	SMB access (for example) from one workstation to another (instead of access to a central server)	X		X	X	

Appendix E – The tree of doctrines: A holistic view of the Defense Doctrine for the organization

To help implement Defense Doctrine and make it accessible to different target audiences, the Israel National Cyber Directorate develops various products/ deliverables to expand professional knowledge in the field. Alongside this, the directorate provides supportive tools that aid in the process.



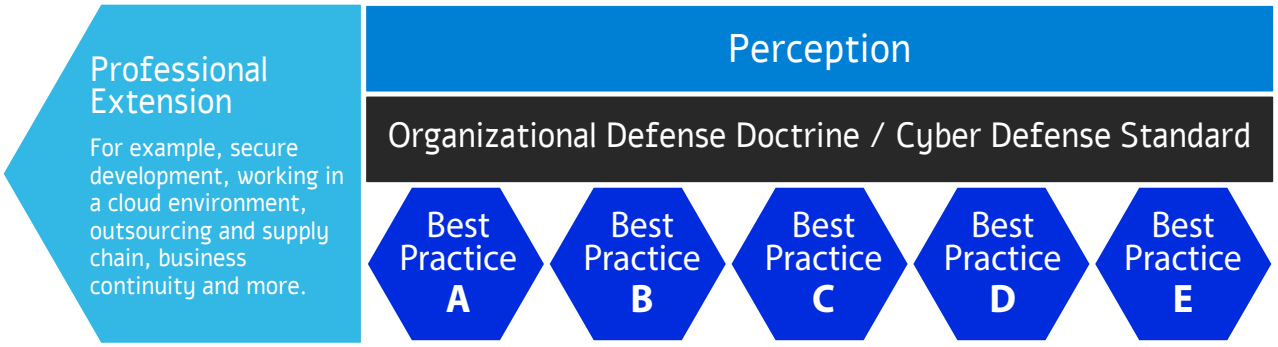
The Doctrine Tree – Defense tools and methodologies that were written by the cyber directorate

The products/deliverables developed by the Israel National Cyber Directorate are available on its website: https://www.gov.il/he/departments/topics/organization_cyber_Defense

In addition, the information is available in the Yuval system – a unique calculator that allows any organization in Israel to easily check the level of its Cyber Defense: https://www.gov.il/he/departments/guides/yuvalrisk

The products that support the implementation of Defense Doctrine can be presented according to the following hierarchy:

- **National perception** – on the basis of which we write the Doctrine of Defense for the organization.
- **Defense Doctrine** – presents the various issues of Defense at the basic level (for example: monitoring, awareness, network separation or supply chain management) and the main things to consider when building an organizational work plan. This document is the professional basis for conducting a risk survey and building a cyber work plan for the organization.
- **Best Practices** – outcomes/deliverables that deepen the recommendations on specific technological issues. These documents present the reader with individual Defense recommendations for implementing Defense Doctrine controls for a particular technology, such as VPN, VOIP, or secure identification.
- **Professional extensions** – products that present to readers the scope of a professional field, and provide them with the broad professional base for access to a project on a particular topic. These products are not focused on a particular technology, and instead present a variety of considerations: How to approach the subject; insights and advice that emerged in the ongoing dialog on the subject with economic bodies; a holistic view of the field; and presenting a concept for implementing the treatment of the issue in the organization. Examples of professional extensions available on the Directorate's website: CISO's work with development bodies, Defense of operating environments, and supply chain risk management.



Appendix F – Data Security & Privacy

Information Defense can have different purposes – for example, preventing damage to reputation, preventing leakage of commercial information, or preventing leakage of private information. While in the eyes of bodies/entities involved with computing Defense the Defense is often the same (such as encrypting a file or setting strict principles for access control), the purpose on the other hand may be different.

The right to privacy was recognized in a Basic Law: Human dignity and liberty, in various laws (chiefly the Protection of Privacy Law) as well as in international conventions. The Protection of Privacy Law includes a number of key principles. One of them is the principle of consent, which expresses the individual's control over the information concerning him – it is he who decides what information will be disclosed, and to whom. This principle is reflected, inter alia, in Section 1 of the Protection of Privacy Law, which states that "a person shall not infringe the privacy of another without his consent." According to the Protection of Privacy Law, consent in this context must be "informed", i.e. one that is given only after a person understands the meaning of his consent and its consequences.

Another key principle is the principle of goal proximity. According to this principle, which is regulated under Sections 2 (9) and 8 (b) of the Protection of Privacy Law, the information may be used only in accordance with the purpose for which it was collected in the first place. Use of the information for any other purpose constitutes an invasion of privacy.

The Protection of Privacy Law, and regulations enacted thereunder, also stipulate various obligations regarding the registration of databases and the manner in which they are secured. Among other things, there is an obligation to examine the need for further retention of information, in accordance with the purpose of its collection.

The Protection of Privacy Law also refers to the rights of the Data Subject. According to section 11 of the law, the Data Subject must be notified of the intention to collect the information, and specify before him what the purposes of its use are and whether he has a legal obligation to provide it – or is allowed to refuse. Section 13 of the Law grants the Data Subject the right to review the information concerning him, and section 14 grants him the right to demand its correction in the appropriate circumstances.

However, like all rights, the right to privacy is not absolute – and there may be circumstances in which other interests will justify a particular violation of it. This concept is regulated, inter alia, in the Defenses set forth in Section 18 of the Protection of Privacy Law. However, such an infringement must be carried out in accordance with the purpose of the provisions of the law and

comply with the general principles of action in reasonableness and good faith – and in the case of public bodies, also the requirement of proportionality.

In general, Cyber Defense is a legitimate action that does not involve any exceptional invasion of privacy. However, its actual implementation should be carried out with in-depth consideration of aspects of privacy and compliance with accepted principles, such as Security by Design, Privacy by Design and Threat Informed Defense. These principles require an in-depth technological-process understanding on the part of the CISO, and he must also know how to strike the right balance between different interests so that its recommendations to the organization's management will enable informed decisions to be made.

Defense Doctrine emphasizes that it is important for the CISO to involve the organization's Legal Adviser already at the initiation and characterization stage of the work plan so as to reduce security disparities. He should later be integrated into key nodes in the information lifecycle of business, business processes and various cyber assets. Thus, for instance, the involvement of the Legal Adviser is required already at the stage of mapping the requirements of the law, regulation, contractual requirements and business needs that the organization is required to meet. All of these form the basis for the existence of the risk management process and the management's compliance with acceptable obligations, such as Due Diligence procedures.

It is also important that the organization's Legal Adviser be a permanent member of steering committees, such as the Information Defense and Cyber Defense Committee. He should also be involved both in employment processes and in contracting processes with the various bodies/entities/parties in the supply chain.

Also, the Defense Doctrine control structure offers the CISO extensive freedom of action. This allows him to reduce the level of risk to an acceptable value, and at the same time minimize the invasion of privacy.

Defense Doctrine emphasizes that the organization must use independent security circles to cope with the various threats (such as abuse of legitimate privileges), and that decision-making must be supported by evidences. As a result, beyond the ability to get a realistic picture of the security situation in the organization (Security Posture), it will be possible to increase the likelihood that actions that infringe privacy will be carried out only in case of real need.

Defense Doctrine also emphasizes the importance of using automation and orchestration processes. This reduces the need for human involvement in the Defense and operational processes, so that the likelihood of human error is small, and at the same time reduces the level of exposure of the various bodies to personal information. For example, by adopting the MITRE ATT&CK

ontology the organization will be able to use advanced automated solutions for continuous and ongoing control and execution of response processes so that human manual involvement will only be required in exceptional cases.

In addition, Defense Doctrine establishes that proactive Defense actions should be taken to preserve information. This is in addition to maintaining effective capabilities for dealing with information leakage events, such as acquiring the ability to remove information that has been leaked to the Internet and Darknet.

In conclusion, it can be seen that the CISO is a significant party in protecting information and privacy, and that he must harness the various bodies within the organization in order to maximize the level of Defense.

Integrating Defense activities in order to improve the level of Privacy Protection in the organization

Defense Doctrine controls are incorporated into a framework, which includes aspects of identification, defense, detection, response, and recovery. Through the implementation of Cyber Defense recommendations and information security, aspects that serve the Defense of privacy are in some cases interwoven into the controls themselves.

Appendix G – An advanced concept of Defense for the organization

The concept of defense required to address advanced threats includes advanced approaches.

Using these approaches will help the organization achieve advanced capabilities, such as validation and deception in order to gain time, exhaustion of the attacker and even creation of deterrence against potential attackers.

These principles may include, but are not limited to:

- D&D – Denial & Deception
- Cloaking and Obfuscation
- Tampering Resistance and Tamper-Evident
- Silence Defense
- Threat Hunting
- Continuous Monitoring
- Diversity/Moving Target Defense (MTD)

The principles of advanced defense can be applied through the adoption of work frameworks and projects such as mitre attack or cyber kill chain approach/ model, and through the breakdown of perceptions into processes and defense routines within the organization.

Here are some examples of components in an organizational concept and examples of their implementation in Defense routines:

Component	Explanation	Purpose	Examples
Exhaustion	Gradual and continuous erosion of the attacker's fighting ability through cumulative damage to his corps/recruits, and to his means and spirit (according to the IDF Glossary)	Changing the viability equation of the attacker in versus the defending body. Raising the walls so that the defending body will not be the preferred target for achieving the purpose of the attack	Performing proactive actions with high frequency to check the integrity of the organization's external/ internal attack surface may enable the detection, identification and treatment of weaknesses before they are abused. As a result, a potential attacker may find that using conventional attack methods (such as Webshell) against the organization is not effective enough. This will require him to develop alternative means of attack (an action that will increase the cost of the attack and prolong it) or prefer to move to a more accessible alternative target.
Cyber Situational Awareness	Ability to produce a good understanding of what is happening in cyberspace and its implications for the continuity of functioning in the organization/economy	Creating a decision-making infrastructure based on a situational understanding of the main threats to the organization's core assets	The Cyber Defense system in organizations often suffers from a constant shortage of resources. An organization that is educated to understand what its Crown Jewels are and what are the latest Attack Vectors that a potential attacker could use, will be able to prioritize Defense efforts more correctly.

Component	Explanation	Purpose	Examples
Deterrence	An action or process of threat, which prevents the attacker from taking action due to fear of its consequences. Deterrence creates in the attacker a feeling that a credible threat is hovering over him, that he has no counter-action for coping with such threat. It is worth noting that the ability to create deterrence depends on the existence of appropriate legal authority, and therefore the ability of the organization to deter in this case will be based primarily on the use of legal and financial instruments. To maintain deterrence reliability the organization must make sure that it activates these devices when needed	Reducing an opponent's motivation to attack the organization	When a user performs an action suspected as being an attempt to gather intelligence before an attack, the message appears on the screen: "You may be performing an action that is defined as illegal – from this moment on, your every action is monitored and documented, and the organization reserves the right to respond by various means." Deterrence may be done by "softer" means, such as legal agreements or Hack Back. In any case, it is mandatory to accompany such an activity with legal advice, due to the inherent risks inherent thereto
Prevention and Fraud (D&D – Denial & Deception)	Using various means and methods to deceive the attacker, and even gather valuable intelligence information. However, actual success depends on the ability to match the means and working methods so as to adapt to the existing production environment or to that which the attacker believes exists.	Gaining time from the moment the attack begins until it is carried out, in order to learn the opponent's courses of action, along with receiving early warning of targeted attack attempts. Along with delaying and learning the attacker, DECEPTION tools make it possible to perform MITIGATION (i.e., ISOLATION or BLOCKING) by connecting to existing tools in the organization (FW, AV, EDR, NAC and more)	This family includes, for example, the use of a Honeypot, Emulator, Honeytokens, Honeynets, Disinformation and Deep Fake. All of these can be implemented in various methods, such as: HONEYPOT FULL OS HONEYPOT EMULATION HONEYDOCS It is also possible to combine at the process level between actions and appearances