



PRIME MINISTER'S OFFICE
NATIONAL CYBER DIRECTORATE
NATIONAL CYBER SECURITY AUTHORITY

CYBER DEFENSE METHODOLOGY FOR AN ORGANIZATION

VER. 1.0





PRIME MINISTER'S OFFICE
NATIONAL CYBER DIRECTORATE
NATIONAL CYBER SECURITY AUTHORITY

CYBER DEFENSE METHODOLOGY FOR AN ORGANIZATION

VER. 1.0

JUNE 2017



\ CONTENTS

Introduction.....	7
Executive Summary.....	10
1. Introduction.....	12
2. The Defense Methodology Tenets.....	14
3. The Defense Methodology 's Structure	15
3.1 The cyclical defense process	15
3.2 Defense Controls Compiled Under NIST Cyber Security Framework.....	16
4. Organizational Planning Process	18
5. The Defense Methodology in the eyes of the organization.....	19
5.1 Implementation of the Defense Methodology for a category A organization...	20
5.2 implementing the Defense Methodology in "B" category organizations.....	24
6. Controls chapters - implementation and control stages	32
6.1 Introduction	32
6.2 How to protect.....	33
Appendices	
Appendix A - Example of risk assessment execution for an information asset.....	134
Appendix B - Toolkit for the implementation of the Defense Methodology	136
Appendix C - Controls for the Defense of a Category A Organization - Highlights for IT Service providers	138
Appendix D - Standards Compliance.....	142
Appendix E - Compliance with ISO 27001	143
Appendix F - Critical protection controls for achieving a high score in a short time...	144
Appendix G - The Controls Bank.....	145

This document has been developed by The National Cyber Security Authority (NCSA) for the protection of Cyberspace in the public interest.

This document constitutes a recommendation for all organizations in Israel.

It can be used freely for enhancing the cyber resilience of the economy.

This document was written for boards of directors and managements of companies, Cyber Defense managers, contractors and IT providers.

The document presents the minimum requirements for protection in accordance with the potential for damage. The protection plan derived from this document should be adapted to the degree of the organization's dependence on cyber.

Organizations are required to perform a risk assessment process and can build a stringent protection program from the requirements of this document.

The document appeals to the entire economy and is written in the masculine form for convenience only.

References to the document can be sent via email to: tora@pmo.gov.il

\ INTRODUCTION

Dear managers, information security and Cyber-Defense specialists,

Cyberspace is the outcome of technological progress, connectivity and a global connection to the Internet.

The increasing dependency on Cyberspace brings tidings of technological innovation and tremendous development for man and his environment.

But alongside these, a threatening space is developing, affecting the business organizations, the integrity of production processes and the confidentiality of corporate information.

Cyber-attacks could harm the organizations and halt the production processes, causing economic damage and harming the reputation of the business.

The State of Israel conducts a national effort for the defense of civil cyber space.

The Corporate Defense Methodology is a component of the National Defense Concept, consisting of various levels of protection on the Israeli economy and its functional continuity.

The Corporate Defense Methodology considers the organization as a whole, and enables raising the level of organizational resilience through continuous integration of processes, practices and protection products.

The application of a Corporate Defense Methodology will enhance the organizational resilience and robustness in face of cyber-attacks.





EXECUTIVE SUMMARY

The purpose of the Defense Methodology is to minimize cyber risks for organizations in Israel.

This document defines a coherent method which guides the corporate responsibility for the construction of a multi-year work plan for the protection of the organization.

Using the method presented in this document, the organization will recognize the relevant risks, formulate a defense response and realize a program to reduce the risks accordingly.

Stage A - the organization will understand to which category it belongs:

- **Category A** - organizations whose resulting damage potential from cyber-incidents is not great.
- **Category B** - organizations whose resulting damage potential from cyber-incidents is great.

The categorization questionnaire appears on page 19.

Stage B - construction of a work plan for the organization

As for the construction of the work plan, the organization will define first what it is required to protect, the required protection level, and the protection gaps in view of the desired situation and will, eventually, construct a work plan to reduce the gaps.

An explanation as regards how to configure the protection objectives of the organization and the level of protection required is presented in this document on page 20 for Category A organizations, and on pages 25-26 for Category B organizations.

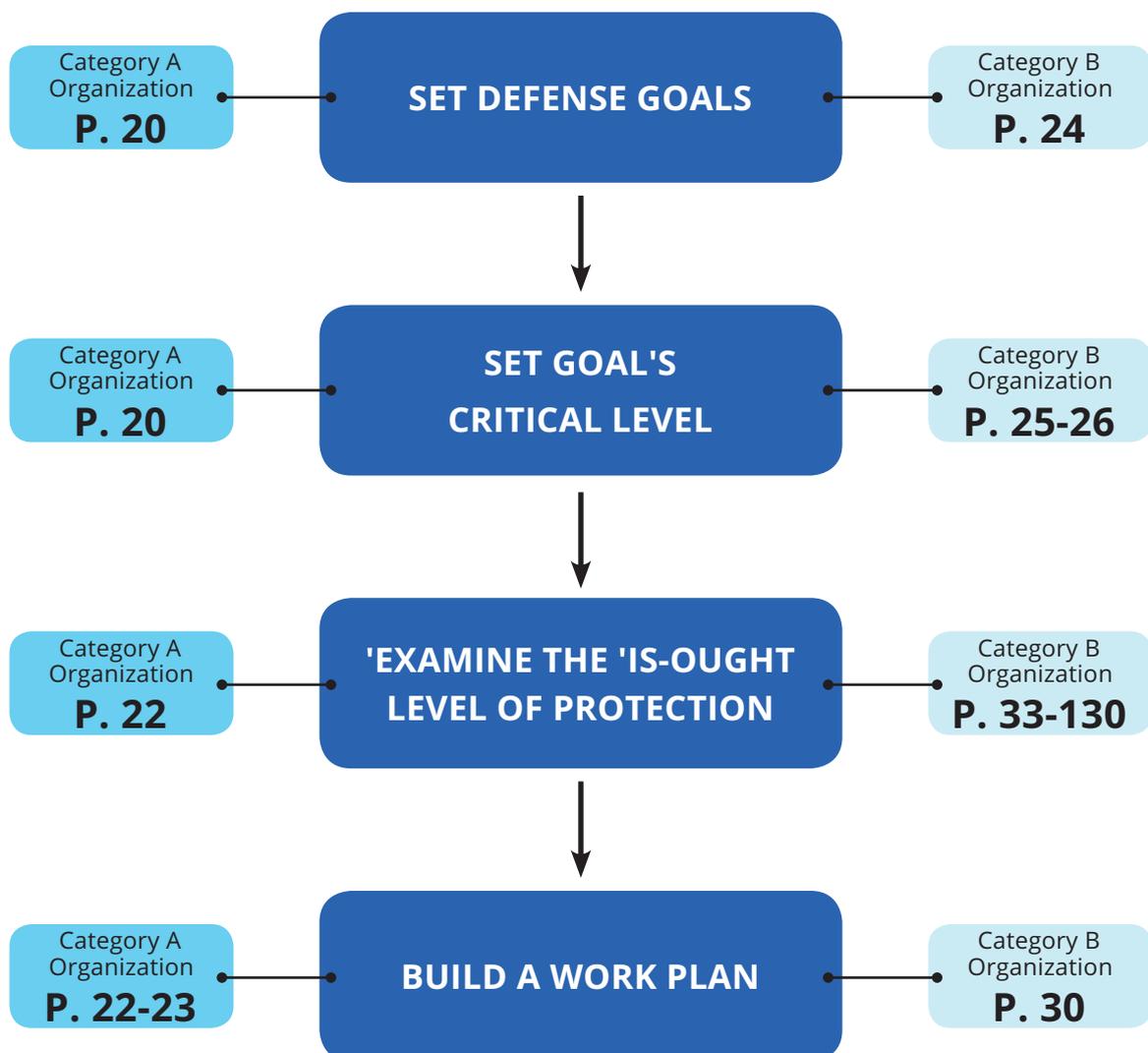
At this point, the organization must understand the controls required of the organization for its various assets. These controls are presented on pages 21-22 for category A organizations, and in pages 33-130 for category B organizations.

The final product in light of the work with this document is:

The organization will understand what are the controls necessary to implement in order to reduce cyber risks to which the organization is exposed.

These controls will constitute the work plan for reducing risks for the organization.

The work plan for organizations that are professionally guided by a dedicated facilitator on behalf of the National Cyber Security Authority (NCSA) , will be built according to the direct guidance of the sector facilitator.



1 \ INTRODUCTION

Cyberspace is an integral part of our lives. On a personal level, we are looking for information on the Internet, navigate our way through road navigation software, talk on a cell phone, and some of us have a pacemaker or an insulin pump connected to the Internet - all part of Cyberspace . On the business level, we use credit cards, manage a customer data base, manage a global organization by computer networks; we market, buy and sell - all based on Cyberspace.

For many of us in everyday life in general and in business in particular, an available, accessible and reliable and constitutes a necessary condition. It is easy to understand this when the above are temporarily withdrawn from us. How will you manage the business without a mobile phone? Without the information stored on the corporate network? Without the ability to execute a credit card clearing?

Cyberspace is a space of possibilities and opportunities on one hand and a space of threats and risks on the other.

An extensive range of state spying, espionage, organized crime and the occasional crime, hacking of personal information and so on is being carried out in this space. These may affect national security (for example, by damaging through Cyberspace a critical national infrastructure, like the power grid or the water system), the conduct of business (e.g., commercial espionage, economic blackmail) and privacy (for example, by posting personal information and images).

Today, various organizations protect themselves from these threats in various forms. The information available online about ways to protect yourself from cyber risks is vast and is composed of methodologies, best practices, 'do's and don'ts', and more.

Protecting the organization against cyber threats requires a lot of knowledge. This knowledge includes a large number of specialties - technological, organizational and procedural.

Many organizations here and abroad are grappling with questions such as - 'Are we investing enough in Cyber-Defense?', 'Do we invest correctly in Cyber-Defense?', 'Do we invest in Cyber-Defense as is common in our industry / sector?' Organizations want to protect themselves and reduce their principal risks in Cyberspace , allowing business activity without fear.

The Defense Methodology helps organizations to map their cyber risks to which they are exposed, to understand the business significance of the realization of the risks and to define proportionate safeguards for the reduction of major risks. The Defense Methodology also defines adequate protection of corporate assets which have an

impact on a sector or which belong to the state level.

The National Cyber Security Authority (NCSA) was established, among other things, in order to design, implement and integrate a national cyber protection Methodology (Government Decision No. 2444). The NCSA has decided, in this framework, to publish the Defense Methodology for organizations in the Israeli economy, starting with government ministries.

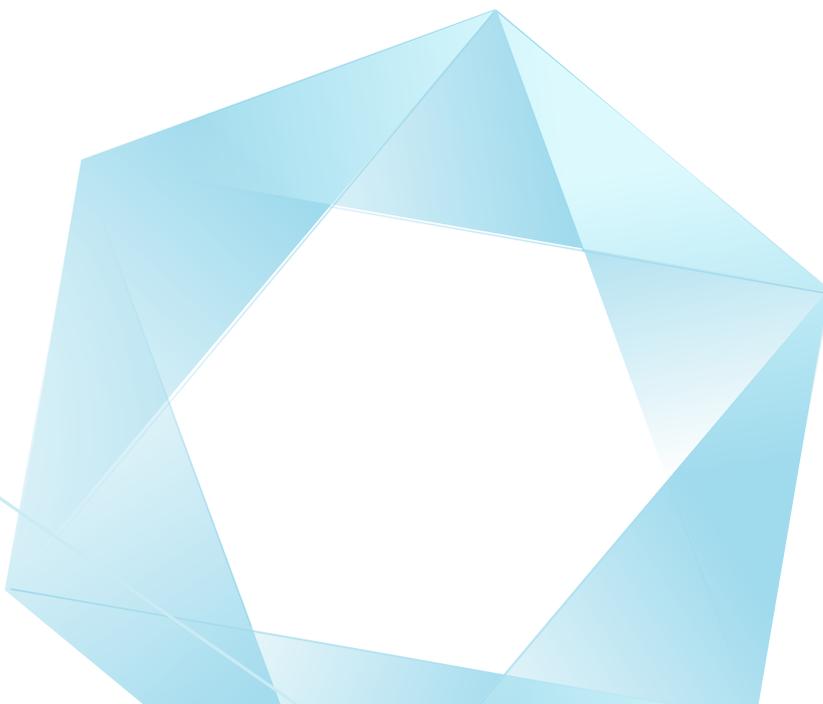
The NCSA has developed this Methodology by combining the world's leading Methodologies, with Israeli civil and security experience, adaptation to Israel's environment and adjusting it to the Israeli business culture.

2 \ THE DEFENSE METHODOLOGY TENETS

The principal protection concept underlying the present Defense Methodology, is the "Organization as a Whole," namely, Recognizing that what is required is a defense of the organization's functional continuity and business objectives.

This concept is expressed in this document in the following manner:

- A. **Management's Responsibility** – responsibility for defending information rests primarily with the organization's management.
- B. **Defense according to potential Damage** – investment in protecting each asset will be proportional to its criticality to the organization's functioning.
- C. **A defense based on Israeli knowledge and experience** – the Defense Methodology enables focusing on risks specific to each organization. The National Cyber Security Authority (NCSA) conducts periodical intelligence reviews and assessments, allowing the focusing of organizations on specific aspects of the various defense circles.
- D. **Proactive Defense** – defense controls were defined, based on the understanding that the organization is required to invest efforts beyond traditional passive defense. This concept finds expression in defining prevention, detection, response, and recovery controls.
- E. **A Multilayer Defense** – defense is a process combining three main components: People & Products & processes (3P's). The Defense Methodology defines a defensive response to each layer.



3 \ THE DEFENSE METHODOLOGY 'S STRUCTURE

Since organizations function in dynamic environments, changes in technology, in companies' character and activity fields influence the manner in which organizations are required to defend themselves in Cyberspace .

The following methodology is based on the fact that the organization is required to assess risks periodically. This risk assessment is the basis of a multi-annual work plan to decrease gaps (implementing required controls).

3.1 THE CYCLICAL DEFENSE PROCESS

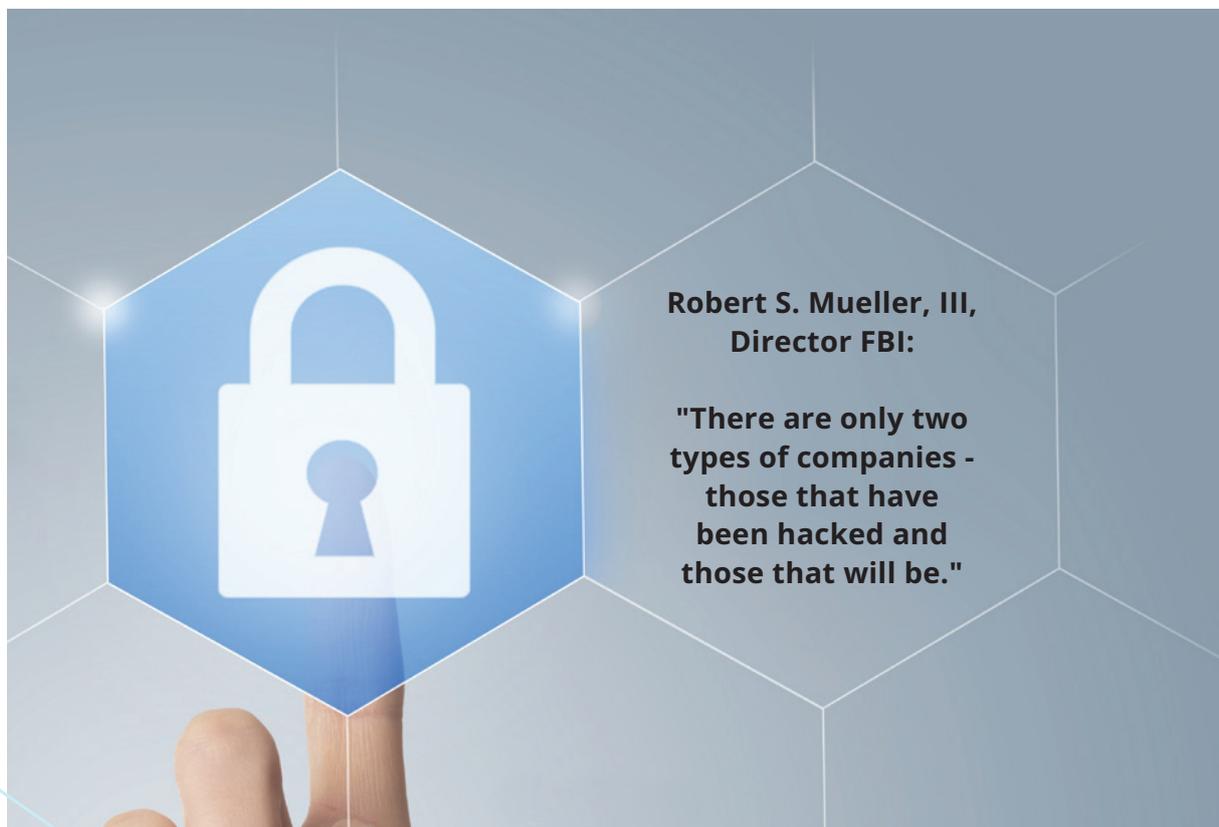
The defense process implied by this Methodology is a cyclical process, comprised of three main stages:

- **Planning and assessment** – mapping the organizational defense objectives, risk assessment, inspecting the existing defense means (controls), and devising a work plan to close defensive gaps.
- **Executing** the work plan by developing organizational processes, tools integration as well as an organizational integration of Cyber-Defense .
- **Maintaining up-to-date defenses** in light of the Cyberspace dynamism in the organization. Processes and technologies integrated in the organization are constantly changing – new computers and networks are installed, advanced software packages are acquired, new elements are linked to Cyberspace, (the Internet of Things, for example), new services are offered (such as cloud computing), etc. On the other hand, threats and attack methods are changing, thus requiring the defense tools - to change as well.



3.2 PROTECTION CONTROLS COMPILED UNDER NIST CYBER SECURITY FRAMEWORK

For many years defense standards emphasized the issue of "defending the organization", namely, **preventing** a penetration of the organization and its cyber assets. **The current reality is different** – organizations of all sizes are attacked, but these attacked only are detected, if at all, after a long time. Therefore, the American National Institute of Standards and Technology (NIST) devised a Framework for Improving Critical Infrastructure Cyber Security, investing both in the traditional preparation and protection phases as well as in the detection, containment, and recovery from cyber-attacks. The present Defense Methodology adopts the NIST Cyber Security Framework, binding together clusters of defense controls. **Within this framework the organization is defended from attack, while its capabilities to detect a successful attack, contain it, and recover with minimum impact are augmented.** These controls are based on international knowledge, adjusted for the Israeli economy, including emphases and examples to assist organizations in focusing their efforts more effectively.



IDENTIFY**Control Cluster:**

- Board and Management responsibility
- Risk assessment and management
- Control, review, compatibility

PROTECT**Control Cluster:**

- Access control
- Data defense
- Defending servers and workstations
- Preventing malicious code
- Encryption
- Network security
- Environment separation
- Cloud security
- Industrial controls defense
- Cellular security
- Change management
- Media security
- Supply chain and outsourcing security
- Purchase and development security
- Human resources and employee awareness
- Seminar

DETECT**Control Cluster:**

- Documentation and monitoring
- Security controls reviews
- Proactive Cyber-Defense

RESPOND**Control Cluster:**

- Event exercising
- Event management

RECOVER**Control Cluster:**

- Business Continuity

4 \ ORGANIZATIONAL PLANNING PROCESS

The planning process is comprised of the following intuitive phases:

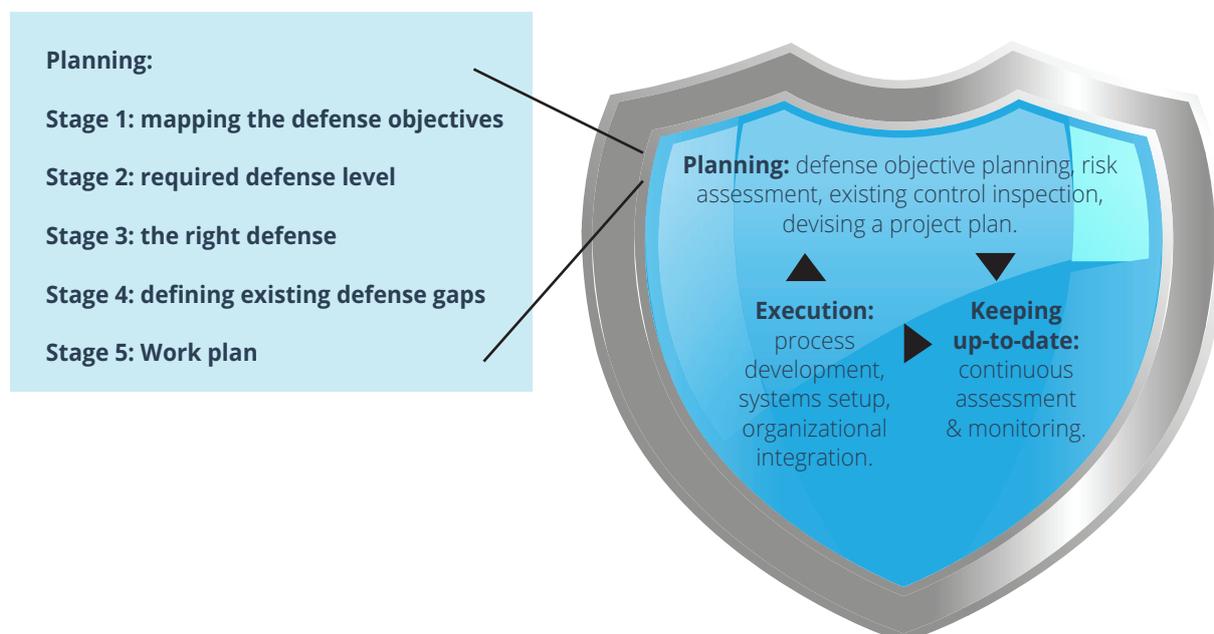
Stage 1: "What is there to defend?" - mapping business assets / processes sensitive to cyber-attacks.

Stage 2: "Impact on the organization's objectives" - understanding cyber-attacks' impact on business assets / processes, by filling a business value questionnaire.

Stage 3: "How to protect correctly" - required controls are derived from the values defined in Stage 3.

Stage 4: Ideal versus real - detecting defensive gaps in relation to required controls.

Stage 5: "Designing a project plan" - improving the defense level in order to reach the desired risk level (including the understanding the essence of the exposure to risk, in case of neglecting to install the required controls).



5 \ THE DEFENSE METHODOLOGY IN THE EYES OF THE ORGANIZATION

This Methodology presents two different levels of recommendations, which are derived from damage potential to an organization due to a Cyber-incident:

- **Category A Organization** - Low damage potential. The organization will carry out a simple process of mapping protection goals in order to quickly understand the necessary protection method required.
- **Category B Organization** - significant damage potential. An organization that relies heavily on Cyberspace and is required to perform a more detailed process.

The division is done after answering the following question:

IF A CYBER-INCIDENT SHOULD OCCUR IN YOUR ORGANIZATION, WILL THE COST OF HANDLING THE INCIDENT BE HIGHER THAN NIS 500,000?

Tip: the cost of damage resulting from a cyber-incident includes direct and indirect damage to the business. These costs include: temporary service shutdown, damage to reputation, cost of sanctions imposed in light of the breach of law and regulatory requirements, and more.

When answering the following question, it is necessary to take into account the total cost. Organizations that responded negatively to the question above belong to category A. Organizations that responded in the affirmative belong to category B.

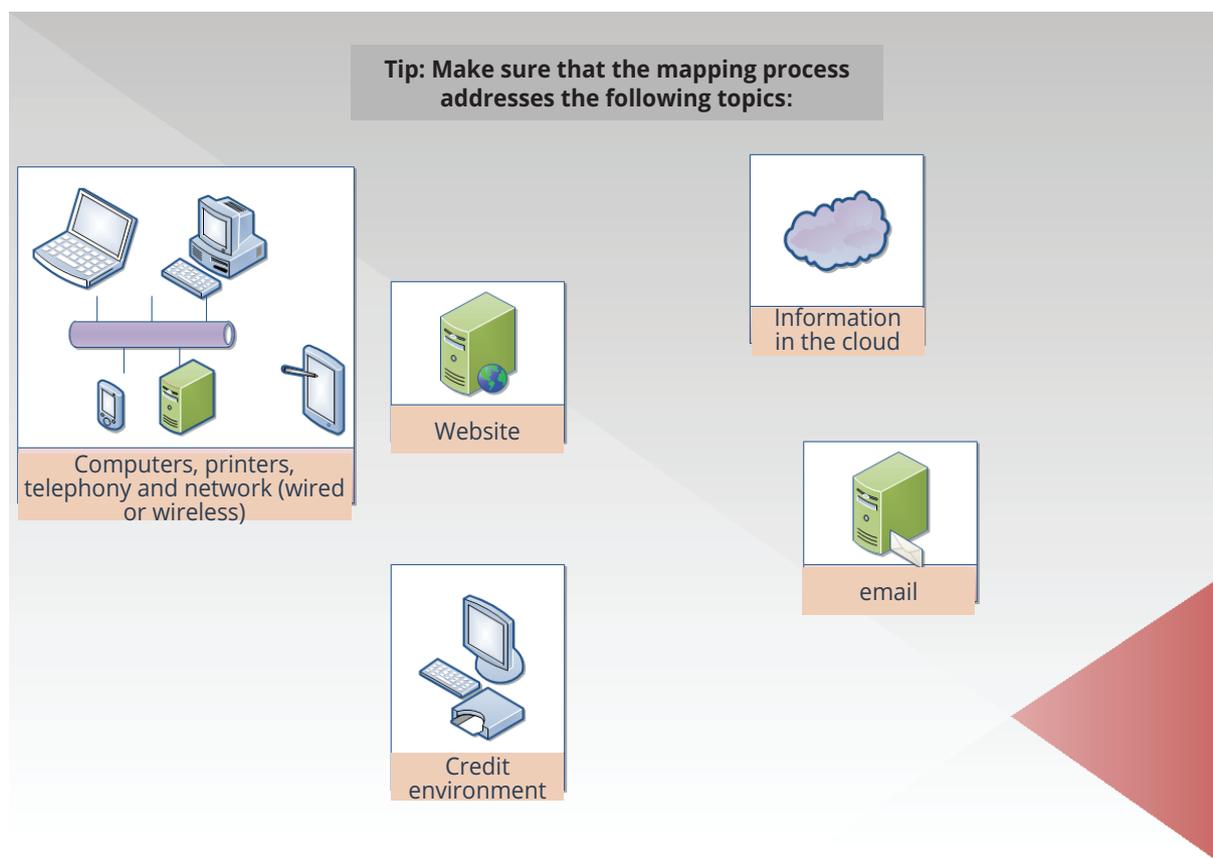
Additional requirements: in case where additional obligations, by virtue of being subject to the existing regulations, apply to the organization, it may be transferred from Category A to category B. In addition, an organization may require its various suppliers to meet requirements of category B organizations.

5.1 IMPLEMENTATION OF THE DEFENSE METHODOLOGY FOR A CATEGORY A ORGANIZATION

The Defense Methodology for a category A organization is confined to pages 20-23 of this document.

Stage 1: Asset Mapping

It is necessary to perform a mapping of major assets. Check with technical support the types of equipment and computing assets used in the organization.



Steps 2 and 3: The Required Level of Protection and how to Correctly Protect - The Ten Commandments for a Category A Organization

A category A organization requires for protection consistent with the damage potential. Therefore the organization is required to implement extremely cost effective controls.

A breakdown of protection requirements is found in Appendix C of this document. These controls are divided into the following ten categories of protection:

<p>1. Management responsibility</p> <p>Understand existing cyber threats, and devise a work plan to close defense cyber gaps.</p>		
<p>2. Avoid malicious Code:</p> <p>Use technologies to cope with malware, and update the organization system defenses.</p>	<p>3. Encryption:</p> <p>Encrypt remote access of employees and suppliers, using commercial encryption means. Encrypt access to sensitive data, use an encrypted communication medium (both from domestic surfing through wireless networks to the organization and vice versa to customers and suppliers).</p>	<p>4. Cloud computing and software purchase: require (contractually) the supplier to comply with common software and data protection standards.</p>
<p>5. Data protection: define protection mechanisms to protect data existing in the organization.</p>	<p>6. Computer protection: define a required computer defense level. Including changing equipment default passwords, removal of unnecessary software programs, redundant connection blocking, removing unnecessary admin accounts.</p>	<p>7. Human resources: instruct new employees and remove former employees' authorizations.</p>
<p>8. Documentation and monitoring: document and monitor exceptional activities, which may attest to cyber threats.</p>	<p>9. Network security: ensure that network access is under the organization's control (suppliers and employees cannot connect remotely at will) and that the network is prepared to withstand denial of service attacks</p>	<p>10. Business Continuity: recover capabilities from site failures, deletion of data, file locking.</p>

Stage 4: Protection Gaps Definitions

A review of the implementation of the controls is set out in Appendix C.

Getting a recommendation from the IT service provider regarding a prioritized work plan for handling gaps.

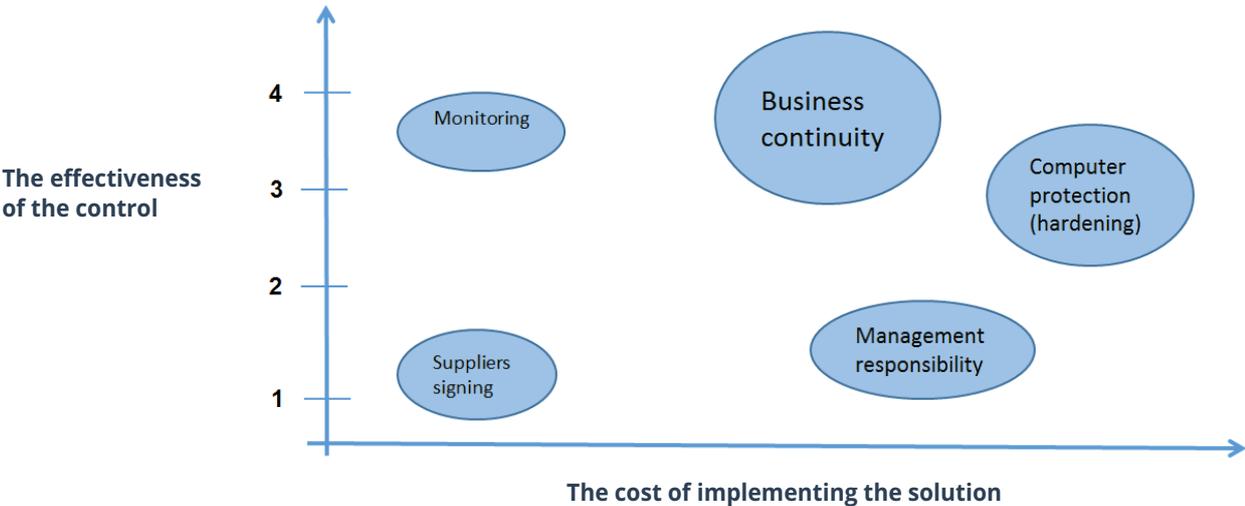
Stage 5: Work Plan

Every control in the controls chapters protects against cyber risk arising from cyber damage. The control reduces the cyber risk which could harm the objectives of the organization.

The program will take the following into account when preparing a work plan for closing controls gaps:

- **The effectiveness of the control** (its contribution to the reduction of risk to the organization)
- **The cost of implementing the solution** - represented below through a 'solution cost' axis (duration of implementation, complexity of realization, required personnel and equipment)
- **Implementation speed** - represented below by the circle size

An example of the weighting of the parameters mentioned above in an organization might look like this:



A lookout table:

Control Cluster	Exists / does not exist	Control effectiveness	Implementation Cost	Data / prioritizing weighting
Management responsibility				
Malware prevention				
Encryption				
Cloud computing and software purchase				
Data protection				
Computer protection				
Human resources				
Documentation & monitoring				
Network security				
Business continuation				

The proposed work plan will be endorsed/approved by the CEO

**A CATEGORY A ORGANIZATION
HAS HERewith FINISHED READING
THE PRESENT DOCUMENT**

5.2 IMPLEMENTING THE DEFENSE METHODOLOGY IN "B" CATEGORY ORGANIZATIONS

Stage 1: Asset Mapping

The organization will map its assets, their functions and interfaces (Web services, API, etc.). Include assets stored in the cloud (XaaS).

The asset mapping Stage should link OT/IT assets to main business processes. Following this phases the organization will be able to distinguish between critical and secondary assets.

This definition will assist in protecting assets in relation to impact.

The asset mapping will include the following list as a minimum:

Type of Asset	Name and manufacturer	Purpose	Local / cloud	Interfaces	Remarks
Organizational application					e.g. DWH, CRM, ERP, WMS, Payroll system, organizational portal, etc.
Infrastructure					e.g. Communication equipment, telephony, Email, storage
Network					e.g. LAN / WAN, wireless, optical, satellite
OT					e.g. Closed circuit television, HMI systems, controllers, etc.

Tip: Assume that whatever you are not aware of is not properly secured. In order to conduct a full IT asset mapping, get a full assets list from the IT department, and work with the purchase department which maintains a full list of products and services.

In mapping OT assets – It is recommended to meet with the operations and security managers (especially in industrial organizations).

An organization that prepared a business continuity plan, may be assisted by the damage assessment and in assessing the dependency of organizational processes on data assets (BIA usage).



Attention: object mapping resolution

Defense object mapping is a time and resource consuming process. In order to carry it out effectively, **attention should be paid to the required mapping resolution.**

For example: on the one hand, one should not specify all servers and terminals, but on the other hand a rough generalization of all servers as one asset may result in disproportionate defense costs.

Stage 2: required defense level

The defense level required for each asset is derived from the latter's organizational value level. Within the defense Methodology, assets are rated at four value levels: 1 notes a low value level, 4 notes the highest value level.



Tip: **common biases in asset value assessment**

Asset value assessment should be conducted in cooperation with business units. An owner may "over value" his asset from the business aspect. But sticking to the value questionnaire's criteria should help assessing assets correctly upon a united, unbiased scale.

At the end of step 2, the organization will be able to define the most important assets to its business activities.

A close cooperation of the business entities within the organization - understanding the business significance of assets and their influence on the business functioning - is required in filling the questionnaire.

**C
I
A**

Attention:

In cyber and data security it is common to assess potential impact by three categories:

- **Impacting data confidentiality** – for example, a cyber-attack intended to leak customers' details to the Internet.
- **Impacting data integrity** – for example a cyber-attack intended to falsify a company's financial reports.
- **Impacting data availability** – for example, a cyber-attack denying information from the company or its customers (shutting down a web site, locking files or planting ransomware).



Define the value level of each asset by filling the following questionnaire:

Question	1	2	3	4
<p>1. What is the level of damage caused to the organization following leakage from the asset?</p> <p style="text-align: center;">C</p>	<p>The damage is estimated at: A) Cost of up to NIS 500,000 to the organization. and/or B) An investment of up to two man-months for handling the incident.</p>	<p>The damage is estimated at: A) Cost of more than NIS 500,000, but less than NIS 5,000,000 to the organization. and/or B) An investment of more than six man-months, but less than five man-years, for handling the incident. and/or C) The asset is defined as a database to whom apply the medium security level in accordance with data protection regulations of the Law, Information and Technology Authority. and/or D) There is a clear danger to public health.</p>	<p>The damage is estimated at: A) Cost of more than NIS 5,000,000 to the organization. and/or B) An investment of more than five man-years for handling the incident. C) The asset is defined as a database to whom apply the medium security level in accordance with data protection regulations of the Law, Information and Technology Authority. D) There is a clear danger to human life.</p>	<p>A significant damage will occur, which will include one of the two scenarios below: A) There is a clear and present danger to the lives of many people. B) The estimated economic damage is over NIS 20,000,000.</p>
<p>2. What is the level of damage caused to the organization following the disruption of information existing in the system?</p> <p style="text-align: center;">I</p>				
<p>3. What is the level of damage caused to the organization following a long-term system shutdown?</p> <p style="text-align: center;">A</p>				

Each asset value score is the highest score received for the three questions (Impact = MAX 1-3). This score is also called **Risk Intensity**. This score defines the maximum damage expected to affect the organization with regards to each asset.

Stage 3: How to protect correctly

In stage 2 we defined for each asset the value extent (intensity) on a scale of 1-4. The degree of protection of any asset is derived directly from the degree of its value (the resulting value raises the intensity level).

Next to each protection control in chapter 6 there is a definition whether it is required for an asset whose intensity score is 1, 2, 3 or 4

For each asset it is necessary to implement the total of all controls whose value is less than or equal to the intensity score of the asset. Thus for example, for an asset whose intensity score is 3 it is necessary to implement all controls whose value is 1, 2 and 3.

This definition helps to adjust the controls required for the application of the defense goal against the damage potential.

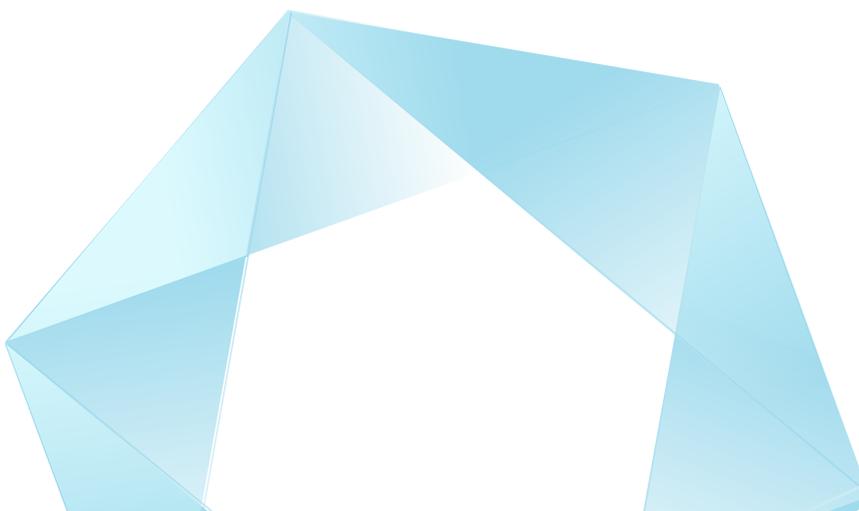
Stage 4: Protection Gaps Definitions

Check what is currently implemented in the organization and what is necessary to perform opposite the protection controls listed in Chapter 6.2. At the end of this process, the organization will receive a list of gaps (gap analysis).

Since not all of the controls are implemented in the same way in an organization, it is important to ensure that the essential protection goals of the organization are examined individually. The reason lies in the fact that a control is not always embedded in every objective of the organization. Experience shows that even though most controls are implemented laterally in organizations, there are not a few cases where a control has not been implemented in a specific system.

Since not all controls are necessary for implementation in every asset, use the value level set for each asset in stage 3 for the benefit of the gap list focus.

This gaps list will be the basis for building the organization's work plan (Stage 5).



Calculating an asset's risk level – weighting the data

Weigh the potential impact (I) with the probability for such a cyber-event to happen.

Probability (P) – calculated by defining an asset exposure level (an asset linked to the Internet, yet having no defense mechanisms, is highly exposed to cyber-attacks, while an asset isolated in a secured room is less exposed).

In order to define an asset exposure level, fill the following questionnaire:

Question	1	2	3	4
1. How many users exist in the system?	Up to 50	50-500.	500-5,000.	More than 5,000
2. Who are the system users?	Internal employees only	Regular external suppliers.	Casual external suppliers.	The general public.
3. How many interfaces exist in the system?	None	1-5.	5-10.	More than 10
4. What is the nature of the system interfaces?	None	Intra-organizational interfaces.	External interfaces with suppliers.	Interfaces to the general public.
5. What kind of information exists in the system?	No business sensitivity.	A company's internal information.	Medical information or customers information.	Sensitive business information.
6. Is there a remote access to the system?	No	Via 2FA	Via an encrypted channel.	Via a commercial takeover software
7. What is the level of compartmentalization permissions in the system?	Full compartmentalization (permissions by groups / roles).	Individual compartmentalization (individual permissions per employee) .	Basic compartmentalization (manager and user) .	No compartmentalization (identical permissions to everyone) .
8. What is the current update level of the system?	The most recent version.	Up to 3 versions back.	More than 3 versions back.	Versions that are no longer supported by the manufacturer.
9. What is the policy for updates and security patches?	Installing full updates at least once a quarter.	Installing security updates only at least once a quarter.	Critical security updates only at least once a quarter.	No orderly updating process.
10. What is the physical security level of the system?	Accessible to unauthorized individuals only.	Accessible to all employees of the organization.	Accessible to external contractors.	Accessible to all visitors to the organization.

The exposure score of each asset is the average score of the 10 questions (P = Average 1-10), also called the risk **probability** (P).

Weighting an asset's risk level, response costs and implementation complexity

In order to calculate the required protection level, multiply by three the impact rating, and add the probability rating: an asset's risk level = (I) * 3 + (p).

				(P)Probability (I) Impact
1	2	3	4	
7	10	13	16	4
6	9	12	15	3
5	8	11	14	2
4	7	10	13	1

An example calculation of an asset's risk is presented in Annex A.

After this Stage, the organization will possess a list that could look like this:

control	The entire organization:	CRM System	Suppliers payment system
4.30 Implement Multifactor Authentication for login of accounts with excessive privileges across the network.	Exists partially	Exists	Required to implement
6.4 Set up and implement security measures to detect and alert on unauthorized changes to configuration settings.	There is an orderly process in the organization	The system is in the cloud and we have no direct control over this requirement	Exists
16.2: Use contractual and legal tools when purchasing an information system or a service from providers.	There is no organized process of signing suppliers in the organization.	The supplier signed a declaration.	This is a supplier from abroad which we are unable to sign. We will consider the requirements in the generic agreement with him.



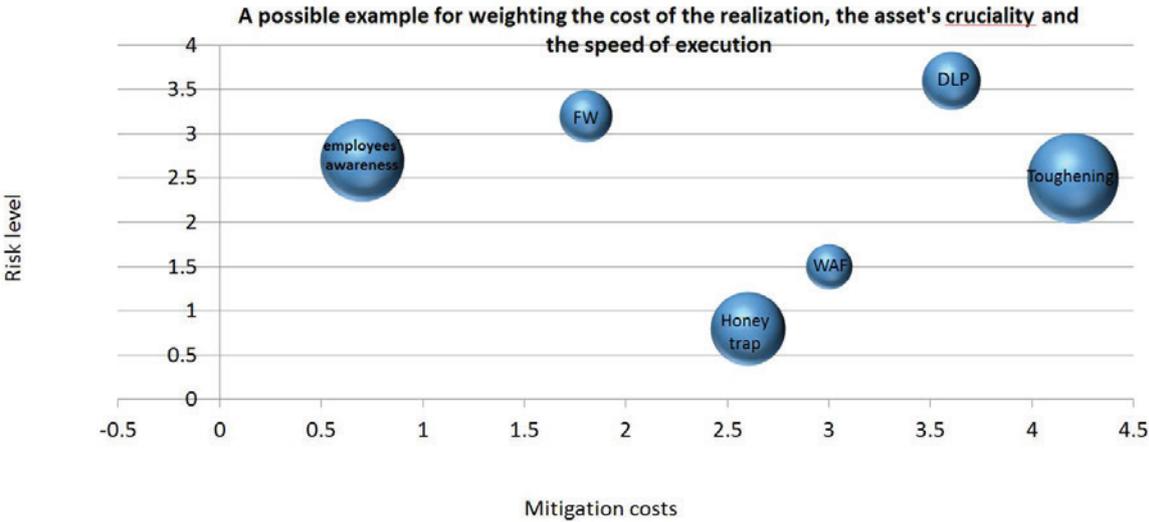
Stage 5: Work Plan

Every control in the controls chapters protects against cyber risk arising from cyber damage.

The priority of application of the controls lacking in an organization in the framework of the work plan will be determined by the weighting of **asset risk level, the cost of the solution and the complexity of the implementation.**

The priority of application of the controls lacking in an organization in the framework of the work plan will be determined by the weighting of:

- **The asset risk level** - Y-axis in the example below.
- **The cost of the implementation of the solution** - X-axis in the example below.
- **The speed of the implementation of the solution** - expressed through the size of the circle in the example below.





6 \ \ CONTROLS CHAPTERS - IMPLEMENTATION AND CONTROL STAGES

6.1 INTRODUCTION

The protection requirements from an organization are called professionally: controls. In order to protect the organization in the cyber field, the organization is required to implement controls in various fields. These controls include the processes, procedures, defense systems and technologies, which the organization has implemented to reduce the risk of the realization of a Cyberspace incident.

These controls are incorporated on the basis of different topics, such as controls for the protection of servers and end stations, user management controls, monitoring controls, and more.



For the sake of focusing, critical protection controls (those with the highest 'cost-benefit' value) have been marked in this document by a Key icon.

For the benefit of construction of a is proportional Defense Methodology the controls in this document are classified in levels ranging on an axis of 1-4, when controls of level 1 are the most basic controls, required from every organization and every asset, while controls of Level 4 are those which are required for a protection target whose potential for harm is 4.

6.2 HOW TO PROTECT

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Identify					
1. Board of Directors' Responsibility. Management Responsibility					
<p>Cyber assets constitute currently critical assets that support organizational objectives. Protecting them can be as important as the protection of physical assets, finances, and employees. Cyber defense is the responsibility of the organization's management. This responsibility expressly requires to be reflected through the perception of Cyber-Defense by the organization's Board of Directors, the Cyber-Defense policy of Management and organizational procedures for Cyber-Defense. Like any defense program, Cyber-Defense is not hermetically sealed, and the Management is required to decide on the level of risk it is willing to take, considering the costs of controls versus the price of the risk materializing within the organization and its impact on customers, suppliers and national targets. Furthermore, the organization's Management must implement mechanisms for handling cyber-events which may occur, in order to reduce the damage to the organization.</p>					
Directorate Responsibility	1.1	The organization's Board of Directors will approve the corporate information security and the Cyber-Defense policy once. year and allocate resources needed for its implementation.	Once. year the Board will be presented with the corporate information security and Cyber-Defense policy, as derived from the organization's cyber risk map. The Board of Directors will approve the risk map and the policies derived from it.	It is recommended to appoint one representative from among the Board members who will be. knowledge focal center (at the managerial level) on the subject. For the benefit of this requirement, it is important to ensure that the risk map is presented to the Board of Directors in. business language alongside the current existing response of the organization and the disparities required in order to reduce the gap and reach an acceptable level of risk. It is important that the Board of Directors will define the risk level that the organization would such as to take ('risk appetite'. for example, as. function of an attribution threat or. cost. benefit) test.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Management Responsibility	1.2	The current risk map as it emerges from the organizational cyber risk survey, should be approved annually.	The organization will map out the risks it is exposed to in the cyber field. The risk will be ranked and presented to Management alongside the definition of the planned response.	Organizations with level. assets can carry out an independent survey by mapping assets and sensitive business processes and work on the basis of the risk assessment method of the Defense Methodology . As regards organizations with protection goals on level. or higher, it is recommended to use an external factor for carrying out the survey period	2
Management Responsibility	1.3	Identify legislation and regulations pursuant to the law, applicable to the organization.	All relevant requirements under the law,. standard,. contract with the organization, and all measures undertaken by the organization in order to comply with the requirement, will be clearly defined, documented, and updated for every information systems and Cyber-Defense activities of the organization as whole.	1. Prepare. list of all the legal requirements, regulations, and contractual obligations that have been identified. An example of statutory and regulatory requirements can be the compliance with the Ministry of Justice (database registration and privacy protection), the protection of credit cards in accordance with the PCI standard requirements, requirements of suppliers and customers for compliance with Cyber-Defense procedures signed by the organization, maintaining copyrights and working with licensed software rather than with pirated one, and more. 2. Perform and document compliance audits, indicating that the above requirements are carried out in the organization.	2

2. Risks Management and Assessment:

An organization's cyber Defense Methodology is based on the process of managing and assessing cyber risks. This is. cyclical process that must be performed when the organization's cyber environment is changing. both within the organization (absorption of new systems, technological changes, changes in business processes, etc.) and outside the organization (constant change of Cyberspace threats to the organization). According to this Defense Methodology. risk management in an organization requires to identify the goals of the defense, define which controls are necessary to protect them and build. suitable work plan.

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Risks Management and Assessment:	2.1	<p>Design. process for setting organizational boundaries, mapping the organization's defense goals and assessing the value level of the defense goals.</p> 	<p>The mapping of the defense goals can be accomplished by mapping the organization's work processes, systems, databases and technological infrastructure. The value level of the defense goals is determined in accordance with the effects of the breach on security, availability and integrity of information.</p>	<p>Defining the goals will include all the aspects where the organization must consider the current risk level against the desired level. These targets may include, among other things, list of systems, infrastructure, business processes, key people and everything that the organization has defined for itself as. Cyber-Defense goal.</p> <p>Please note that there are defense goals which were added in recent years and by mistake have not been mapped. Good mapping will include, for example, the IOT world, including security cameras, elevators and electrical stairs, assembly and other 'software integrated' components, which often are not managed by the organization's IT professionals (do not constitute classic IT assets). These assets are often at the heart of the action of the organization's operation and are no less vulnerable to cyber-attacks (such as an amusement park Ferris wheel, fuel pump, central air-conditioning system, command and control system for turbines, etc.)</p>	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Risks Management and Assessment:	2.2	Define and implement. periodic cyber risk assessment process in accordance with the organization's threats outline, the level of exposure to threats of the defense goals, and the protection controls implemented in the organization.	The purpose of the risk assessment process is to provide an updated map of the actual cyber risks (residual risks) in order to define. plan to address the risks. The survey must be carried out periodically and must be updated following changes in processes and systems in the organization.	It is possible to base the risk assessment process on the Cyber-Defense Methodology .	2
<p>3. Monitoring, Reviewing and Compliance: Every organization is required to protect its cyber assets in order to comply with basic legal aspects of copyright protection (for example, not using unauthorized software), to protect corporate records and protect private information which is located in the company's database. Coded information, if there is any, is kept in accordance with the relevant rules of the legislature. Some organizations are required to meet additional legislative requirements. The organization must build control mechanisms to verify on an ongoing basis that it meets the requirements of the law, the relevant regulation, according to the sector (health, insurance, capital markets, etc.), this Defense Methodology. the Board policy and Management decisions regarding aspects of Cyber-Defense.</p>					
Control, Review and Compliance	3.1	Review periodically the various information processes for the purpose of ensuring compliance with security standards, policy and any information security requirement.	A 'Management survey' of the various processes must be carried out, to confirm compliance with the standards and Information Security requirements. This survey will examine the various parameters in the field of Cyber-Defense and provide Management with. snapshot regarding the organization's strengths and weaknesses.	A Management survey provides lateral vision on the state of the organization in terms of its current level of protection. These surveys will present to the organization the areas in which it is required to focus, vs. areas in which the organization is more mature (such as the CMMI maturity model). The areas that the survey can refer to might be, for example, secure development, level of awareness, monitoring capabilities, maturity level of response teams, organization procedures, etc. It is important to ensure that the processes defined as critical in the framework of the organization's business continuity program are given proper protective response.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Control, Review and Compliance	3.2	The organization will ensure the writing of. protection policy, which will address all aspects detailed herein.	The purpose of the monitoring is to ensure that the organization's Management has defined its guidelines regarding protection aspects of various topics, such as human resource protection policies, supply chain protection policies, monitoring and control policy etc.		
Control, Review and Compliance	3.3	Make sure that the various information systems comply with corporate information security. Cyber-Defense standards, and that they are implemented securely on. regular basis. in accordance with the corporate information security and Cyber-Defense policy.	Periodic reviews should be carried out in order to ensure that the various information systems comply with the information security and Cyber-Defense requirements that the organization has set and that they are immune against attacks.	The proper implementation of this monitoring will be carried out by writing an annual or multi-year corporate plan for performing periodic cyber surveys on corporate assets. The surveys can be in the form of. white. gray or black box, while prioritizing the review of systems that received. high score in the values questionnaire. As regards level. systems, it is recommended that the review be carried out by an independent body outside the organization.	2
Monitoring, Auditing and Compliance	3.4	Automatic check of the organization's level of protection.	Use automated tools, which simulate the attacker activity automatically.	Since performing penetration tests is an action that requires for the most part human involvement, the ability to cover many systems in real time is limited. For the benefit of addressing time and knowledge limitations, there are some products that enable the Director of Defense to receive notification using tools that simulate. 'war game', attacking the organization using various methods in order to detect attack vectors and weaknesses to address.	4

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Protect					
4. Access Control:					
<p>Many factors require access to the organizational information for proper functioning, both human elements (the organization's employees, customers and suppliers) and technological factors (applications). These require access to different systems and information types. In order to prevent abuse of this access, the organization must implement monitoring and protection which will ensure that anyone can access only the information they need, and that it is not being used by an unauthorized party. It is also required to ensure that the accessing parties are identified and verified unequivocally. For this purpose, it is required to manage the various users (human and applications) on an ongoing basis, add, abolish or change their privileges as appropriate and record their activities. Extra caution is needed in providing elevated privileges to people and applications (many attacks make use of impersonating parties with elevated privileges) and to detect the corporate network remotely. Access control is one of the basic areas of Cyber-Defense of the organization and requires care for detail.</p>					
Access Control:	4.1	Develop, document and implement an access control policy.	The access control policy is designed to ensure that only authorized parties can access the organization's information and systems to view and make changes, all in accordance with the definitions of their roles and subject to supervision.	The organization's access control policy may be included as a chapter of its information security policy	2
Access Control:	4.2	Set up user accounts that support the business functions of the organization. 	At the very least, separate the 'Administrator' account from 'user' account. It is also necessary to set up users who manage the system security functions (such as creating users, managing access and system privileges, managing the information security systems, etc.).	Creating corporate users as standard users, assigning 'administrator' users per defined function only (administrators).	1

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.3	Examine the list of users periodically and update it accordingly.	The organization will examine every pre-defined period the list of users and remove irrelevant users as needed.	The periodic users review process and its documentation using access control procedure organizing, ongoing monitoring through an automated or manual array, will be performed by systems administrators. This review is conducted in order to identify both inactive users. users who have left the organization and to ratify the privileges of existing users. For example, if an employee has moved to another position in the organization, in many cases he is 'dragged' with the previous privileges.. review of the business side by the system administrator may float such cases.	2
Access Control:	4.4	Disable. remove temporary accounts automatically after. specified time. 	The organization will set. fixed time period, after which temporary account will be blocked automatically.	If possible, set up temporary accounts with. time allocation for any system that interfaces with an Active Directory or. management system or an Identity Management system (IDM). Accounts that must be extended require. special approval.	3
Access Control:	4.5	Disable. remove inactive accounts automatically after. specified time.	The organization will disable. remove inactive accounts after. fixed period of time, defined in the policy.	Periodic reports must be issued regarding users' login activity in system that interface with an Active Directory as well as accounts that were closed. long time ago (as defined in the access control procedure.) Delete such accounts.	3
Access Control:	4.6	Document in an automatic log record any creation, modification, enabling, disabling, and removal of accounts.	The organization will document any change to user accounts and will conduct an automatic or manual follow-up of the execution of the documentation.	This can be implemented through monitoring (SIEM), which will interface with per task management systems in the organization. Active Directory, IDM, servers, applicative systems as well as communication and information security equipment.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.7	Monitor account activity in order to detect anomalous usage and report unusual use to the appropriate officials.	Examples of anomalous use: Logging into the system on certain days and at certain times, login from addresses incompatible with normal use pattern.	Can be applied using SIEM system for monitoring users in sensitive groups. The information collection will be made from sources such as Active Directory, communications and information security equipment (firewalls, etc.).	3
Access Control:	4.8	Define and enforce conditions for blocking accounts.	Examples of entry blocking conditions: Weekend, night hours.	It is possible to define in the user setting an entry restriction on the Active Directory account, so that the restriction will not allow connection during non-working hours.	4
Access Control:	4.9	Define and enforce logical access privileges to the system and the information in accordance with the access control policy.	The access control can be done on the personal level (identity-based), or the role level (role-based), and aims to control the access of entities (users or computer processes) to objects (files, records, devices etc.).	Users will be managed centrally through an organizational Enterprise Directory, e.g. an Active Directory, Open LDAP and more. The per task system will be mapped to the user profile.	1
Access Control:	4.10	Limit user privileges to the essential minimum to perform their duties.	The organization will define minimum level of privileges for each role as well as minimal privilege level for basic user (without defined role) required for access to the organization's systems.	User privileges will be in accordance with their role. basic profile will be defined and given to the user, and additional privileges will be granted according to need and with the approval of direct supervisor; if there is an IDM system basic profile and applicative profiles can be mapped. After improvement of the process privileges will be given depending on the role.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.11	Define officials, carry out. separation of duties and give it expression through granting system privileges.	The purpose of the separation of duties is to reduce the potential for abuse of privileges. The separation includes, for example, separation of business functions between employees or officials, as well as ensuring that the information security team that manages the access control does manage the access control Review functions at the same time.	A per task mapping which supports. separation of powers must be carried out and implemented within user privilege profiles, e.g.. developer vis-à-vis. software tester (each of them will have access to. different environment:. developer will work in. development environment. a low environment;. tester will work in. higher environment. pre-production), etc.	3
Access Control:	4.12	Access to sensitive systems and applications will be made only through. designated mediation hardened component (Terminal).	For the benefit of applying. uniform 'hardened' policy to sensitive resources, ensure that access to them will be made only after going through the mediation component (such as. proxy server or terminal).	It is possible to exercise this control by defining access in the firewall component so that connection to sensitive assets is permitted only through the link component, including testing and the stringent corporate policy (such as preventing the ability to perform 'copy. paste', preventing download files capability, CLI locking, etc.) .	4
Access Control:	4.13	Define employees who are authorized to publish information in. system accessible to the public (such as. Web site), and implement this authorization as part of the privileges granting process.	The organization will define users whose job require the ability to publish information on public sources and will document the above-mentioned functions as part of the organization's procedure.	In Content Management Systems (CMS), it is necessary to grant editing rights and publication privileges only to content managers.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.14	Restrict user login to the system after several unsuccessful login attempts using the lock option to log in for. specified time, or until. release by. system administrator.	The purpose of this monitoring is to deal with the risk of Denial of Service attacks. This control must be implemented at both levels of connecting to the operating system and of connecting to specific applications.	It is possible to limit the number of failed login attempts within the Group Policy and the Domain Policy.	2
Access Control:	4.15	Limit the number of simultaneously-allowed connections of. single user.	The purpose of this monitoring is to detect the connection from two different places using the same identification. Such. scenario might be an indication of unauthorized use of. user account.	It is possible to limit the number of simultaneous connections in the Remote Logon policy in the Group Policy.	3
Access Control:	4.16	Lock connections resulting from temporary inactivity and disable the continued connection until the identification and re-authentication of the user. As part of the connection locking hide information that has appeared on screen prior to the locking.	This control is usually applied at the level of the operating system, but it can also be implemented at the application level. It should be noted that. connection locking is not. regular substitute for log-out.	This can be achieved by setting. screen saver. If possible, make sure that self-development systems and shelf products systems include. Session Time Out mechanism.	3
Access Control:	4.17	Write down and implement usage restrictions and configuration requirements for remote connection. 	A policy for handling remote connections is required, which defines the limits of the use of remote connection to the organization's resources. The use of systems that provide secure remote access to the organization's resources is required as well.	It is possible to implement secure access to the organization through systems such as VPN or SSH, which are consistent with corporate policies for remote connection to enterprise resources.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.18	Remote connections should be monitored.	Automatic monitoring of remote connections allows organizations to detect cyber-attacks. as well as allowing to ensure compliance with remote access procedures by controlling the activities carried out during the remote connection.	It is possible to interface the remote access systems with monitoring systems such as SIEM, and verify that login events are indeed recorded. Special emphasis should be placed on remote login by external suppliers to the organization for maintenance and support, and on monitoring their activities effectively (e.g. Through monitoring and screen-recording tools).	3
Access Control:	4.19	Route all remote connections through. set number managed network access control points.	Reducing the number of access control points reduces the attack surface.	Review the organization's attack surface mapping and transfer sensitive corporate services to the network area located behind the firewall. Redirect traffic to it from the VPN network through access from the VPN server. Eliminated direct extra-organizational to access these services.	3
Access Control:	4.20	Implement additional safeguards when executing sensitive commands via remote connection.	Sensitive commands are, for example, booting, server or cancellation of. transaction. Make sure that it is impossible to execute such commands in the framework of. normal login system.	Access to sensitive servers as well as to the systems management will be carried out by an Out-of-Band management network, which can be accessed through. dedicated management server (requiring identification and authentication).	3
Access Control:	4.21	Prohibit remote login in order to manage the system, and limit access to the system from networks that are not managed by the organization.	The organization will not allow direct remote access to management interfaces, unless securely, and only after verification and connecting to. management network.	Administrator Login must be avoided when remotely connecting to systems (can be done in Linux also by eliminating PermitRootLogin).	4

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.22	Protect the connection to. system from. wireless network using user. devices authentication, encryption and setting usage limits.	The organization will allow connection to. wireless network only for devices managed. authenticated by it, and only for identified users. The purpose of this monitoring is to prevent illegitimate and unidentified use of the wireless network.	Access to the wireless network will be allowed only after identification opposite the Access Point.	2
Access Control:	4.23	Calibrate the signal strength of the wireless signal in order to reduce the chances of signals will be received outside the organization's facility.	The organization will review the broadcast signals of the wireless networks and will ensure that the signal does not exceed. predefined range.	Mapping of the reception range can be carried out using spatial overview and special equipment (Radio) in coordination with the wireless system provider. It is also possible to conduct independently via Radio Analyzer and scanning around the area of the building.	4
Access Control:	4.24	Prohibit connecting to organizational systems from. wireless network.	Access to enterprise systems will be allowed only for computer equipment through. wired connection to the organization's network.	Do not connect the wireless networks to the organization's network, but only on. dedicated Internet router for surfing only. It is also possible to implement. proxy server of the wireless network.	2
Access Control:	4.25	Write down and implement usage restrictions and configuration requirements for connection through mobile devices.	The organization will write down and implement. policy for monitoring information security for mobile devices that access the organization's systems. The policy should address both the devices provided and managed by the organization as well as personal devices of the organization's employees or guests.	Write down. mobile devices policy, which defines the limits of the use of mobile devices (such as cell phones and tablets): what can be saved and accessed in the organization via. mobile device.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.26	It is imperative to implement full encryption of the information stored on mobile devices in order to protect the confidentiality and integrity of the information.	The organization will encrypt the disk space of mobile devices that connect to conduct its systems.	This can be applied through. policy which will be distributed to mobile devices using Mobile Device Management and supported by the majority of Android and Apple devices.	3
Access Control:	4.27	Ban logging into sensitive system through mobile devices.	The organization will block and enforce through technological controls access to sensitive organizational systems via mobile devices.	This can be applied by identifying the mobile device's browser, or, alternatively, do not allow the exposure of sensitive systems to networks accessed by mobile devices (neither behind the VPN segment, or, alternatively, to connect mobile devices to. VPN segment that is different from the other computers).	4
Access Control:	4.28	It is necessary to identify and validate uniquely the users of the system.	The organization will verify in an unequivocal manner. user connecting to the organization's systems.	Each system user will have. unique username (which is mapped to. particular person). As for generic user, it will be indicated who has the generic username and applicative users will be owned by the system administrator.	2
Access Control:	4.29	Implement Multifactor Authentication for login to accounts with excessive privileges across the network.	The organization will implement local identification by several identification means (two or more) in sensitive accounts.	Can be realized, for example by using magnetic cards, fingerprints or other mechanisms supported by Active Directory.	2
Access Control:	4.30	Implement Multifactor Authentication for local login of accounts with excessive privileges.	The organization will implement identification by several identification means (two or more) in sensitive accounts in local login.	Can be realized, for example by using magnetic cards, fingerprints or other mechanisms supported by Active Directory.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.31	Implement an authentication mechanism which is replay-resistant for connecting each account (with an emphasis on verification mechanism by encryption means).	The organization will implement an eavesdropping-proof identify mechanism (such as an identity mechanism which issues one-time identification) for all accounts.	Can be realized through mechanisms such as smart cards or one-time password.	4
Access Control:	4.32	Implement Multifactor authentication to connect remotely to the system.	The organization will implement remote identification by several identification means (two or more) for the organization's systems.	Can be realized through mechanisms such as smart cards or one-time password in remote access to systems such as VPN.	2
Access Control:	4.33	Identify and validate uniquely devices which are in the progress of connecting.	The organization will recognize unequivocally devices connecting to the corporate network.	Can be realized by using digital certificates issued to end point and portable computers.	3
Access Control:	4.34	Manage means of identification to the system, including: selecting means of identification of an employee or office holder and their placement and blocking after period of disuse.	Manage pool of identification methods and their issuance. Also, It is possible to cancel the means of identification through central system.	Can be realized through OTP management system if it stronger identification means than the existing system is required.	2
Access Control:	4.35	The organization must enforce password policy through technology.	The policy enforcement must include at minimum: setting minimum complexity, variance from previous passwords, set expiration time, requirement to define new password after an initial login.	Can be realized by using Group Policy and Domain Policy.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Access Control:	4.36	Ensure that the feedback from the information system throughout the verification process does not provide information that could cause harm if discovered or if it will be used by unauthorized parties.	Disguise the authentication fields by hiding the password.	Can be realized through built-in mechanisms in the operating systems. It is also possible to implement in Web pages by defining the field as. Password.	2
Access Control:	4.37	Implement encrypted authentication mechanism.	The goal is that the identifying information will not be exposed (Clear text). Exposed identification information can be stolen if transferred through an unencrypted communications medium, for example, in case of an MIDM attack.	Can be realized through mechanisms such as smart cards or one-time password.	2
<p>5. Protecting the information:</p> <p>In the digital age we live in, information is one of the most significant assets for most organizations. whether it is business information, customer data or any data collected and maintained by the organization for the purpose of its business operations. Accordingly, the organization must act to protect its information from theft, tampering, or deletion, and sometimes it is even obligated to do so under the provisions of the law. These controls apply to protecting the information itself. its classification, storage, portability and so on.</p>					
Protecting the information:	5.1	Prevent unauthorized or unintentional data transfer via shared system resources. 	The organization must prevent the transfer of information in an unauthorized manner, e.g. by using shared folders, email, removable media etc.	Restrict the use of shared folders for transferring information, especially when there are also per task to unauthorized parties. It is possible to use. DLP system in order to prevent the transfer of information stored in shared folders.	1

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Protecting the information:	5.2	The organization must write down and implement relevant policy and procedures to protect the information and update it periodically.	The policy must include at least reference to various types of information in the organization system. The policy must include clear definitions about taking out information beyond the boundaries of the organization, and the method of releasing that information. In addition, it is necessary to refer to all the channels and terminal equipment in the organization: workstations, servers, mobile equipment, including computers, tablets, mobile phones and wearable computing equipment (smart watches, etc.).	This control can be implemented by writing policy document regarding the protection of information in the organization. The document must include definitions for the various types of information in the organization, what types of information can be sent outside the organization. Furthermore, it is also necessary to write complimentary procedures on how information is sent securely.	2
Protecting the information:	5.3	The organization must write down and implement an organizational information classification policy and implementation procedures for the organization's employees for the purpose of labeling the information.	The classification policy must include clear definitions of how and in what way to classify each type of characterized information.. procedure for guiding how to handle each classification of information should also be added.	1. Characterize the types of information available in the organization according to their importance. based on business needs, or rules and regulations applicable to the organization. 2. Produce. matrix that includes all of the classification categories. what is included in every classification (i.e. What types of information, for example: private, business, health, public security, etc.) and the different types of information handling (storage, transfer, destruction, physical and logical protection, etc.).	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Protecting the information:	5.4	Implement safeguards to prevent information leakage when transferring information to internal or external parties.	The organization must implement mechanisms for the protection of information when moving between enterprise systems and when sending it to parties outside the organization in accordance with corporate information protection policy.	Can be realized using several technologies, each of which may prevent certain scenario: 1. An information leak prevention system; 2.. secure system for transferring information such as secure. encrypted email, an electronic safe etc.	2
Protecting the information:	5.5	Implement protection mechanisms for monitoring and preventing access, use or removal of information, defined as sensitive by the organization, to unauthorized entities within and outside the organization.	The organization must implement mechanisms for the protection of information while saving it in the organizational storage arrays, which may be physical, virtual and cloud servers, as well as when safeguarding the organizational workstations; ensure that the protection mechanisms do not allow replication, printing, sending, deleting, etc. of information defined as sensitive information contrary to the policy established regarding that information.	Can be realized using technologies to prevent information leakage in order to monitor, warn and prevent these actions. Can also be implemented using document protection solutions (Document Security) as well as through monitoring and restricting access to sensitive files (expanded on in the chapters on access control and monitoring).	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Protecting the information:	5.6	Prevent remote operation of computer accessories (webcams, microphones, speakers, headphones, or any accessory that may be connected to PC) and provide an explicit indication regarding the fact that computer accessories are physically active with the user.	Prevent blocking, disabling remote operation of cameras, microphones and so on.	It is preferable to permanently block computer accessories which are not used in order to reduce this risk.	3

6. Protection of workstations and servers:

Workstations and servers are the basic computing equipment in any organization; protecting this equipment is fundamental to prevent attacks on the organization and protecting corporate information. Workstations and server protection controls have several layers of protection. Toughening Services (White. Black List), preventing the creation of security breaches by using both maliciously and accidentally, and more.

Protection of workstations and servers:	6.1	Define, document and implement. toughening policy for workstations and servers, which meets the requirements of the organization's information security.	The organization will define toughening requirements for systems within the organization with an emphasis on what are the basic requirements, the frequency of updates and the level of classification and then document the requirements in an overall framework which will serve as basis for toughening procedures.	It is possible to use baseline documents of the official manufacturers and standards organizations, such as DISA, SANS, etc.. Also, define in the organization's procedures who is responsible for the implementation of the actual toughening and how the ongoing test of the controls is carried out. The toughening documents shall include, inter alia, reference to the usage of unauthorized. safe services, approved ports, removal of inactive accounts and so on. It is important to make sure that the toughening will be carried out in accordance with the relevant functionality of the application (such as toughening IIS servers opposite TOMCAT, WEB server toughening opposite. DB server toughening etc.).	1
---	-----	--	--	---	---

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Protection of workstations and servers:	6.2	Implement mechanisms for centralized management, implementation and validation of the system configuration.		On Windows systems It is possible to use Group Policy tools such as Active Directory; in Linux systems It is possible to use, for example, Red Hat's tools, or, alternately, management and auto configuration distribution tool like Chef.	3
Protection of workstations and servers:	6.3	Set up. policy to control, enforce and monitor the installation of software on the organization's PCs.	The purpose of the control is to make sure that the software is installed on endpoints and servers only with approval and after examination of the need and risk involved in using the software.	This control can be realized by restricting user accounts for installation. modification of the software endpoints as well as by using an Application Control tool.	2
Protection of workstations and servers:	6.4	Set up and implement security measures to detect and alert on unauthorized changes to configuration settings.	System configuration changes may reduce the level of protection of the asset. Thus, for example,. change of password length setting, or per task to install software that is not in accordance with the organization's policy exposes it to risk.	Can be achieved by defining relevant laws in the SIEM system by comparing periodic reports (current versus previous configuration), by means of dedicated monitoring and control tools that provide an indication of the configuration changes, etc.. It is recommended to adopt CCM (Continuity Control Monitoring) tools in order to receive notification in real time.	3



Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Protection of workstations and servers:	6.7	Set up and use. Whitelist of permitted-to-use software and block any other software.	The organization will define. list of permitted-to-use software and will block installation and use of any other software using the organizational configuration management system, or by using. third party tool and will block the installation of these software programs.	It is possible to set up. list of permitted-to-use software using the Active Directory, or using configuration management tools. Some of the servers and endpoints protection tools support the above capabilities.	3
Protection of workstations and servers:	6.8	The organization will conduct monitoring of servers and systems which have been excluded (and whose exclusion was approved) from the implementation of. hardened configuration.	Sometimes, for business and. or operational reasons it is impossible to apply the level of protection for all assets in the same way. In such cases, the organization is required to implement. process which will require special per task to exclude. particular server or system from information security requirements following. certain need, and in doing so the organization will be responsible for providing compensating controls instead of exclusion.	It is possible to set up. sector head or an official who will constitute an 'Approving Authority' for exclusion from the policy for the benefit of the exclusion needs, will examine the operational and business need for exclusion and recommend compensating controls.	3

7. Preventing Malicious Code:

Malicious code is being used by hostile elements to the organization and is designed to penetrate it without the approval of the organization in order to harm it through Cyberspace (data theft, data tampering, damage to computer systems, etc.). Malicious code is. broad term, which includes many types of abusive software: viruses, worms, Trojans, Rootkits, Adware and more. System protection against malicious code is of paramount importance in the Cyber-Defense of an organization. The defense array includes prevention of malicious code intrusion on one hand (at entry and exit points of corporate communications, servers and endpoints), detection and the process of handling malicious code that has infiltrated the organization, on the other hand.

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Preventing Malicious Code:	7.1	<p>The organization will activate tools and systems in its external communication points. These tools will scan and detect malicious code. These tools will operate on communication with external parties, email and browsing services.</p> 	<p>The purpose of this monitoring is to detect malicious code prior to its entering the organization, still at the GW level.</p>	<p>Can be realized by using proxy servers, NGFW systems and tools dedicated to different communication protocols, such as email.</p>	2
Preventing Malicious Code:	7.2	<p>The organization will define procedures for handling stations, servers or networks infected by malicious code.</p> 	<p>The purpose of this monitoring is to ensure that the organization is prepared to cope with malicious code infiltration events.</p>	<p>Examples of procedures: procedure for detection and removal of malware, operating system re-installation procedure, identification of trends and reaching conclusions in the case of. massive propagation and infection in the organization.</p>	2
Preventing Malicious Code:	7.3	<p>Implement tools to detect and prevent malicious code on endpoints and servers in the organization. These tools will be run in an active protection mode and periodic scans will be performed as well.</p> 	<p>Since some abusive software may penetrate the security mechanisms, ensure that controls for handling malicious code will also be applied at the workstation level.</p>	<p>It is possible to use any tool to detect and prevent malicious code (such as antivirus) from. recognized manufacturer.</p>	1
Preventing Malicious Code:	7.4	<p>The organization will implement and manage these capabilities as part of the endpoints protection tools, or will integrate tools with these capabilities in addition to existing antivirus tools.</p>	<p>The purpose of this monitoring is to raise the level of detection and handling of endpoints 'beyond' the basic capabilities of an existing antivirus system.</p>	<p>HIPS products can be used independently or as additional capabilities of software protection of anti-virus products.</p>	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Preventing Malicious Code:	7.5	Advanced controls must be activated to prevent malicious code in the operating systems of servers and endpoints.	The organization will activate in the operating system mechanisms that make it difficult for malicious code to access memory or operating system functions.	Can be achieved with solutions for identifying anomalies in the operating system level.	4
Preventing Malicious Code:	7.6	Implement. tool for identifying malware at the network level.	The organization will activate tools that will be implemented at the organization's network with the aim of identifying and alerting of online malware propagation.	Examples of these tools: Honeypots, Anti-Bot technology, IDS components etc..	3
Preventing Malicious Code:	7.7	The organization will manage the malicious code prevention tool in the organization through. central system. The main management tools will enable. major reporting of suspicious incidents and system events identification (problems updating, protection inactive, component removal, etc.).	The purpose of this monitoring is to manage effectively the protection system from malicious code. Working through locally installed configuration makes it difficult to distribute updates, to ensure full coverage and to control the overall defense situation.	Most malicious code prevention systems allow the use of management tools with. centralized management interface.	2
Preventing Malicious Code:	7.8	The organization will activate detection and prevention measures, based on the detection of behavior which deviated from reasonable and acceptable behavior, in addition to the use of electronic signatures based tools.	The purpose of this monitoring is to detect activities that deviate from the norm. The encryption of multiple files, documents that attempt to access the registry files etc., are for example events which are supposed to raise. 'red flag' in the organization.	It is possible to use tools that analyze heuristics,. user or. system's behavior.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Preventing Malicious Code:	7.9	Run an automatic updating of all systems for identifying and preventing malicious code within the organization. 	The organization will activate automatic updates from. central server, managed by the organization or by. recognized service provider. These updates will keep the protection tools constantly updated.	It is possible to use update servers, embedded within the organization's management servers as part of these systems, or, alternatively, use the manufacturer's servers If there is no central update server in the organization's network (also applies to cloud services).	1

8. Encryption:

Intelligent use of encryption is of great help in protecting the information and preventing its exposure, even when it had leaked, thus reducing much of the business significance of information leakage. It is therefore important to define applications that require encryption and the encryption type required, in accordance with laws, guidelines, procedures, regulation, business commitments and the economic feasibility in the framework of risk management. It is imperative to configure encryption on different media information may leak from (memories, communication middleware, etc.) and to define mechanisms for the managing and monitoring encryption (such as management of cryptographic keys and digital certificates in various stages). Of particular importance is the media encryption on mobile devices (laptops, mobile phones, tablets, etc.).

Encryption:	8.1	Define uses that require encryption and the encryption type required, in accordance with laws, guidelines, procedures, regulations and business commitments.	The organization will define what information and systems should be encrypted and record the configuration of the information encryption. The requirements will be derived from the requirements applicable to the organization or from information retention requirements.	Examples of such requirements are laws protecting privacy, PCI-DSS, and other security requirements.	1
Encryption:	8.2	Manage and protect encryption keys during production, distribution, storage, access and destruction.	The organization will define procedures and processes for the issuance of encryption keys, protecting the private encryption keys and servers for issuing keys and certificates, toughening procedures and procedures for rekeying.	Toughening and preserving the Root Ca Servers, protection using HSM, cryptographic key distribution to systems and employees, operating the PKI array.	1

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Encryption:	8.3	Ensure the availability of information even in the event of loss of encryption keys.	The organization will implement an encrypted data recovery system through the implementation of managed processes and appropriate tools.	For example,. laptops disk encryption recovery array by using the manufacturer's disk encryption tools and managed recovery processes.	3
Encryption:	8.4	Implement encryption of sensitive information transmitted between the organization's systems and end-user interfaces on public communication middleware.	The organization will implement data encryption arrays for sensitive information displayed to the user through. browser,. mobile app or other systems that provide access to information through public networks such as the Internet.	Using approved and updated SSL certificates in the browser.	TBD
Encryption:	8.5	Implement encryption of sensitive information transmitted between systems within the organization.	The organization will implement encrypted traffic in interfaces between servers and services that transmit sensitive information and will prefer to use protocols which encode traffic.	Can be realized using protocols such as SSL, SSH, HTTPS, and more.	TBD
Encryption:	8.6	Implement encryption of sensitive information transmitted between the organization and external interfaces, vendors, external systems. 	The organization will implement encrypted communication with suppliers and systems outside the organization.	Can be realized using protocols such as SSL, SSH, HTTPS, SFTP and more.	2
Encryption:	8.7	Implement encryption mechanisms on portable devices' media (laptops, mobile phones, tablets, etc.).	The organization will implement hard disk encryption of mobile devices and portable media devices.	Mobile devices and tablets can use the manufacturers' disk encryption system. Other operating systems can use the vendors' tools which enable disk encryption.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Encryption:	8.8	Use encryption mechanisms based on recognized encryption algorithms and key sizes corresponding to the outline of the threat.	The organization will not use encryption mechanisms with known weaknesses and vulnerabilities, and will match the encryption strength, including the encryption key sizes, to the outline of the threat.	For example: do not use outdated encryption methods, such as SHA1, SSLv1, SSLv2, or encryption keys smaller than 128 Bit, etc.	2
Encryption:	8.9	Manage. digital certificates array for the issuance and revocation of digital certificates and use digital certificates from trusted sources only.	The organization will manage an array for the issuance of digital certificates and an array for the revocation of certificates (CRL). In addition, it will also use external certificates issued by trusted sources only (Trusted CA).	Can be realized through an orderly and up-to-date CRL server array, and the use of external certificates from approved services (Trusted CA).	2
Encryption:	8.10	Define. process for the renewal of digital certificates prior to expiration.	The organization will ensure that the digital certificates in regular use are renewed prior to their expiration. If the certificates are replaced. older certificates are distributed to certificate revocation servers (CRL).		2
Encryption:	8.11	Carry out periodically. proactive replacement of sensitive encryption keys.	The organization will define the life of sensitive cryptographic keys and take care to replace them in time. It is also necessary to implement. replacement process of encryption keys in sensitive applications.		2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
<p>9. Network security: The communications infrastructure of the organization is a key factor connecting all computing resources at its disposal, both among themselves and to the Internet and to other organizations. The communications infrastructure is critical to everyday activities in many organizations, and its shutdown or damaging it has significant meaning for the organization. Therefore the organization's network is a starting point for many types of attacks on the organization, and consequently it is imperative to protect it against internal and external threats. Network Protection includes functional, technological, processing and procedural separations, control and monitoring of networks, filtering and blocking suspicious information, and more. Extensive network controls, because many attacks are carried out through the corporate network. Great importance is given to controls designed to protect corporate networks connection among themselves, corporate communications nodes and of course with the Internet.</p>					
Network security:	9.1	Write down and implement communication network protection policy, Review and update it periodically. 	The organization must write down and implement network security policy. The policy should include reference to topics such as access channels to the public Internet network and configuring their protection. In addition, it should address core aspects of internal communications and external communication.	Writing policy document or its integration as a chapter in the organization's information security policy.	2
Network security:	9.2	Separate user functionality from network management services.	Management interfaces are to be separated from other user interfaces in order to reduce their exposure to unauthorized access to management interfaces.	Can be realized through a separate login page for users and for administrators. A separate communication network used to connect to the equipment management interfaces. Restricting IP address authorized to access the management interface and so on.	3
Network security:	9.3	The organization will operate technological devices in order to protect services against Denial of Service attacks.	Defend against Denial of Service attacks (DOS) of various types, such as loading the computing resources to collapse, loading the communication bandwidth, loading the website to crash and more.	Control can be implemented using tools such as firewall systems (using an IPS module), intrusion prevention systems (IPS), application firewalls (WAF), as well as restrictions on the amount of volume of traffic towards certain systems, or limiting the number of queries performed on the system.	1

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Network security:	9.4	Disconnect network connection linked to the session at its conclusion, or after. specified time of inactivity.	The organization will apply limits on the lifetime of the connection, and will monitor and break communication without trans task.	Control can be implemented using. firewall and setting it so that network connections receive. Timeout after. set period of inactivity.	2
Network security:	9.5	Set guidelines for the use of IP telephony technology (VOIP) and also monitor its use.	The organization will define when and how it is permitted. prohibited to use VOIP services (embedded in the organization's systems or as an external service) and will operate information security measures in order to enforce those settings.	Can be applied by Separating the VoIP network from the standard network, limiting non-telephony connectivity equipment to the network using measures such as NAC, identification of the equipment opposite VOIP servers as well as the use of encryption and identification using SSL.	2
Network security:	9.6	Make sure that the Address Translation Service (DNS) is provided by. trusted server (intra-enterprise and extra-enterprise.)	The organization will allow the obtaining of Address Translation Service (DNS) only from. secure internal server, in order to prevent erroneous communication routing (intentionally or unintentionally) to hostile targets.	Internal DNS servers will be configured and will provide. response to the organization's servers. It is also possible to configure dedicated DNS servers for more secure areas of the network.. Enterprise servers will be configured so that any request to. DNS service will be performed solely through those servers	1
Network security:	9.7	Make sure that the answers received from the address translation server are reliable and were not altered during the transtask..	The organization will ensure that answers returned from the address translation server cannot be modified through mechanisms such as underwriting answers that are sent by. digital certificate.	Can be applied using DNSSEC extensions of the DNS service.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Network security:	9.8	Protect the communications credibility at the session level, so that both ends of the session will be sure of the correctness of the identity of the second party (MITM protection, session hijacking, etc.).	The organization will activate reliability monitoring through technology such as digital certificates while establishing communication between various system services.	It is possible to use SSL certificates for identifying the service and. secure internal CA server which issues certificates for the various services in the organization. The service is supported in an Active Directory infrastructure and Microsoft's Kerberos services. The session management monitoring can be applied using session monitoring at the server level (such as IIS or Apache), or at the network level using Load Balancer.	2
Network security:	9.9	Monitor the organization's outbound. inbound network traffic. 	The purpose of this monitoring is to ensure that traffic into and out of the organization will be permitted only in accordance with the defined policy (access through authorized protocols, approved service, from. to approved destinations, etc.).	Can be realized through the application of firewalls which distinguishing between the enterprise's network and external networks.	2
Network security:	9.10	Monitor and control major communication junctions within the organization's network.	The organization will divide its network into sub-networks, according to risk level. data classification in the systems.	The networks can be separated through. corporate firewall between environments, setting up environments such as. buffer zone (DMZ) for services outbound to the internet, management networks which will be connected behind. secure connection, networks that contain sensitive services and sensitive systems.	3
Network security:	9.11	It is necessary to limit the number of communication channels outside the system.	The organization will reduce and unite communication channels to ensure better control over the connections to the system.	Using. terminal server to connect to the system.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Network security:	9.12	Block by default all network traffic and allow manually any desirable traffic by means of exception rules. 	The organization will define the filtering rules of network traffic so as to block by default all traffic not explicitly defined as allowed.	Configuring 'Zero rule' in the firewall, blocking all traffic not explicitly enabled. Make sure that routes are set up so that all traffic will be routed through firewalls.	1
Network security:	9.13	Prevent devices from creating local communication over the system in parallel to communication via an external connection..	The purpose of this monitoring is to prevent. situation where the computer acts as. bridge that connects the external world to the internal network of the organization.	It is possible to configure the workstation by. policy that determines that only one network card is active at any time on the server, connections will be configured only to the hub of the organization, behind. firewall, while eliminating other network cards (which are not connected to. required network by definition, such as storage network), such as wired. wireless network cards.	2
Network security:	9.14	Communication should be routed within the organization to external networks through authenticated and managed proxy servers.	The organization will determine that all communications to external networks will be made only through proxy servers. In order to create. medium which will prevent direct communication that exposes the organization's resources to the Internet, and also in order to facilitate implementation of concentrated controls and protections of communication channels versus the Internet.	Can be applied via. proxy server connected to the world, while surfing is performed only through it. The proxy server will be configured with the option to restrict connections to unauthorized sites and categories. Also, servers will be configured so that Internet access is enabled only for updates through the proxy server (if it is impossible to use. dedicated updates server of the system manufacturer).	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Network security:	9.15	Implement mechanisms to prevent unauthorized physical connection to the corporate network.	Connecting unauthorized equipment to the enterprise network exposes enterprise resources to damage of confidentiality and integrity of information and computing resources and their availability.	Can be implemented through using NAC systems.	2
Network security:	9.16	It is necessary to apply mechanisms that filter communication that does not match the structure of the expected protocol information.	These mechanisms must be implemented in order to defend against malicious use of insecure, unlicensed protocols. Also, ensure that communications packages arrive in the correct configuration and have not been altered before reaching the destination.	For example, traffic filtering that does not meet firewalls standards, XML Firewalls Application.	3
Network security:	9.17	Make sure that in the event of operational failure of one of the border protection devices (firewalls, etc.) the system security level is not compromised.	Information security equipment must be configured to block communication in case of failure.	Most of the information security equipment can be configured so as to give redundancy toward the secondary equipment (secondary firewall for the benefit of redundancy, another secure communication route, etc.), and if there is no redundancy, the failure will move the system into Fail-Close status.	2
Network security:	9.18	Border protection mechanisms must be used to separate system components that support business tasks or services, defined by the organization as requiring separation.	The organization will determine that the separation of networks into secure areas will be carried out through dedicated information security equipment.	It is possible to use tools such as firewall, VPN tool allowing to connect securely to management networks, access control at the router level, proxy servers.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Network security:	9.19	Use separate network addresses (different sub-network) to connect to different security zones.	The organization will determine that each sub-network will have. separate address range, which will be published to the firewall and routers.	Can be realized through centralized addresses management on the central firewall management interface, or through manual registration (managed and controlled) of the different network addresses.	1
Network security:	9.20	Implement mechanisms for maintaining the integrity and confidentiality of the network traffic on. public medium.		For example, encrypting outbound traffic outside of the organization, communication lines encryption on. public medium.	2
Network security:	9.21	Define, document and implement. toughening policy for communications equipment, which meets the requirements of the organization's information security.	The organization will define toughening requirements for the communication systems within the organization with an emphasis on what are the basic requirements, the frequency of updates and the level of classification and then document the requirements in an overall framework which will serve as. basis for toughening procedures.	Baseline documents and references to the requirements of toughening in the policy documents. Also, define who is responsible for the implementation of the actual toughening and how the ongoing test of the controls is carried out. The toughening documents shall include, inter alia,. reference to the usage of unauthorized. safe services, approved ports, removal of inactive accounts and so on. It is important to make sure that the toughening will be conducted in accordance with the manufacturer's recommendations. Toughening recommendations can be found in accepted industry standards, such as DISA, SANS and the official website of the manufacturer.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Network security:	9.22	Implement mechanisms for centralized management, implementation and validation of the communications equipment.		Can be applied by type of telecommunications equipment and according to the central management mechanism of any manufacturer. Also, it is possible to apply the various media components toughening manually by using the management interface of each component separately.	3
Network security:	9.23	A mechanism (central or local) for managing firewall policy.	The organization will define the firewall systems management policy, which will include reference to the process of adding, removing illegal routing rules in the system, including an approval process to add, remove rules. It is also necessary to set up the manner of documenting and detailing as regards any rule that opened in the firewall for its proper management.	Can be implemented directly in the system management interface. It is possible to apply, process of approval for opening, removal of rules, as well as the creation and actual removal of rules in the system by using automated change management systems.	2
Network security:	9.24	Improvement of the firewall rules. 	The organization will carry out, process of reviewing the rules of the firewall system and improving them, in order to maintain system integrity and for confirming that there are no rules which could expose the organization to unnecessary risks.	Can be applied mechanically using automated systems to manage the changes, or, alternatively, perform, manual process of examining rules and definitions.	3
Network security:	9.25	Periodic network scans. 		Can be performed using free scanning tools, such as NMAP, Superscan others.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
<p>10. Separation of Environments: An enterprise network can include several environments, such as: production environment, development environment, testing environment, management environment and more. These environments are often linked together, while also differing in the type of information that exists in them, the required level of availability, in their management and in the level of defenses and information security controls embedded in them. As such, attackers exploiting weaknesses in the less protected environment in order to obtain a foothold in the corporate network and use it to attack the more secure environments. In order to protect workspaces, the organization must create a separation and a barrier between different environments through physical separation (at the level of communication, storage, virtualization, keys management, etc.), control over information transfer between environments, separation of users and their privileges, information and software transfer processes between environments, integration of security tools, filters and monitoring tools.</p>					
Separation of Environments:	10.1	Write down and implement. Separation of Environments policy, Review and update it periodically.	The organization will write and implement a policy of separation of environments, such as production, development, testing, support, Internet, guest network environments, etc. The purpose of the separation is to prevent the ability to move between environments by utilizing the access permissions or shared infrastructure.	The policy should contain: definition of the environmental types of separation, the separation level required (e.g. Logical or physical separation) and referral to appropriate procedures.	2
Separation of Environments:	10.2	Configure separate environments for development, testing and production. 	The organization will define and delineate the environments that need to be separated in order to prevent leakage of cyber-incidents between the environments in case of damage to one of them.	Definition of different environments, mapping systems and technological demarcation (networks, servers and databases) of each environment.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Separation of Environments:	10.3	Restrict the use of sensitive production data (customer data or data defined by the organization as sensitive) in non-production environments if they are not protected at the same level as in. production environment.	Since the lower environments are accessed by developers and quality assurance personnel in. less controlled manner, there is concern that sensitive data will leak out. In addition, the level of security in these environments usually based on. lower security level than in the production environment. In order to reduce exposure due to the access of developers and others to the test and integration environments, it is necessary to prevent sensitive data transfer in these environments.	It is possible to use anonymization processes (task or data scrambling identifiers), or. synthetic test data for development and testing environments.	2
Separation of Environments:	10.4	Separate user privileges for various environments and define the privileges for each environment separately. 	It is necessary to manage users and privileges in. single user management system, however, it is necessary to set up. separate privileges registry for each environment separately, so that environments containing sensitive information would not be exposed to unauthorized access in case of hacking. user account or abusing privileges.	Setting up. separate user account for the employee for any environment in which he is required to operate. Access privileges will also be defined separately for each account, depending on the business need of the employee.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Separation of Environments:	10.5	Set up an approval process for data transfer from the production environment to other environments and set up. process for secure data transfer.	The transfer of sensitive data from the production environment to other environments is sometimes required as part of the development and testing processes. In order to prevent abuse of these processes, it is necessary to implement. controlled data transfer process, which requires appropriate approvals prior to execution.	Can be applied using. mechanized process, including approval by information security factors.	2
Separation of Environments:	10.6	Set up. controlled process of software component transfer from the development and testing environments to the production environment.	Implement software components transfer process to the production environment, designed to ensure the completion of testing procedures and obtaining appropriate approvals before executing the transfer.	Can be applied in the framework of 'Going-to-Production Committee' which concentrates changes in the production environment and their approval before executing the transfer.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Separation of Environments:	10.7	Separate environments that implement different security level in. manner that takes into account the level of threat posed to the 'more secure' environment than the 'less secure' one.	Production environments tend to be carefully managed and have wide controls and safeguards, while development and testing environments tend to have looser management and contain fewer controls and safeguards. To avoid damage to the production environment due to the utilization of weaknesses in low environments, set the different systems and environment security levels and separate environments that implement different security levels.		2
Separation of Environments:	10.8	Apply the separation between environments in the telecommunications network, storage systems, virtualization, identification processes and management of encryption keys.	A complete separation between environments requires the application of separate physical networks and separate infrastructures. Using shared infrastructures requires the implementation of mechanisms of separation from suppliers, adapted to the level of threat and the nature of the risks posed to the technology environment		3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Separation of Environments:	10.9	Implement bidirectional filtering mechanisms in communications and data transfer interfaces between environments, to prevent passage of malicious code, attacking weaknesses, applicative interfaces exploitation and uncontrolled release of information.	A complete separation between environments requires the application of separate physical networks and separate infrastructures. Using shared infrastructures requires the implementation of mechanisms of separation from suppliers, adapted to the level of threat and the nature of the risks posed to the technology environment	Can be realized via advanced filtering technologies that enable content filtering and advanced filtering rules.	3

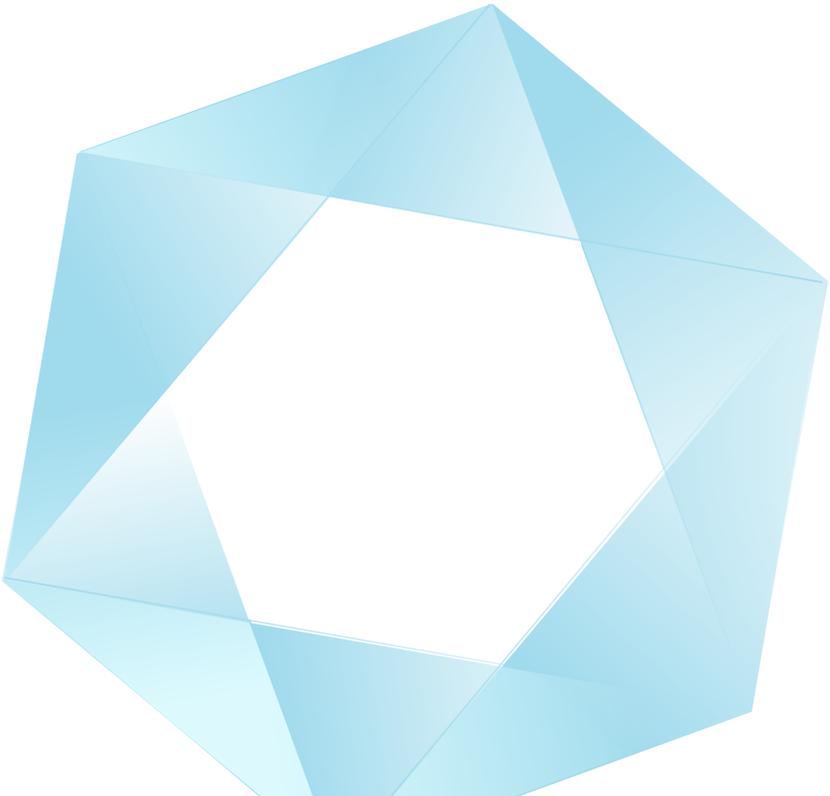
11. Public cloud computing:

Many organizations rely increasingly on cloud services for processing and storing information. Alongside the advantages of the move, the organization is required to manage the resulting risk of valuable information for the organization being transferred to. third party (the cloud service provider). Therefore, it is the duty of the organization to ensure that the cloud services do not affect the level of its Cyber-Defense. by setting appropriate requirements to the cloud service provider. The organization has to understand the security services division of responsibilities between the service provider and the organization, and implement protection monitoring accordingly. at both the enterprise and provider level. The organization is required to ensure that the cloud service provider undertakes to comply with standards and regulations required from the organization, conduct the appropriate Cyber-Defense controls for information value and to define appropriate control processes. The business continuity plan of the organization is required to take into account situations of revocation of the ability to access cloud services. Ensure that the cloud service provider implements mechanisms for information security monitoring and reports to the organization regarding exceptional events.



Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Public cloud computing:	11.1	It is necessary to understand the division of responsibilities between the service provider and the organization, and implement protection monitoring accordingly.	When using public cloud services there is. division of responsibility of cyber protection between issues under the responsibility of the supplier and issues remaining under the responsibility of the customer. This division of responsibility depends on the nature of the service and the implementation model. The organization has to understand what are the issues that are within its responsibility and implement the consequences of this responsibility.	In the case of services such as PaaS or IaaS infrastructure, the client responsibility is to manage the users, to monitor usage by users, manage the data and ensure its security, secure applications and interfaces and often secure operating systems and infrastructures. all depending on the nature of the service, as defined in the agreement with the provider. These controls can be implemented using monitoring and control tools provided as part of the service, using the tools available in the organization or by external suppliers, which provide cloud security services.	1
Public cloud computing:	11.2	Write down and implement. policy for usage and protection of public cloud services, Review and update it periodically.	The organization's management must define. policy and guidelines as regards the conditions and rules for the use of public cloud services and the manner by which the organization implements Cyber-Defense in the event of use of public cloud services.	A policy on the use of cloud services deals, generally, with the following issues: What are the services that may be used in the organization, what are the specific requirements of the organization, topics that include contracting with suppliers, privacy risk management, supervision and control. When writing this policy take into account the legal requirements regarding outsourcing, published by The Israel Law, Information and Technology Authority (ILITA).	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Public cloud computing:	11.3	Make sure the cloud service provider undertakes to comply with the required standards and regulations, depending on the organization's obligations and standards agreed with the provider.	Various organizations are subject to regulatory guidelines relating to the use of cloud services, such as privacy protection, sectorial regulation or contractual liability to third parties. These obligations often dictate strict rules for the use of cloud services.	For example: the implementation of the Bank of Israel directives, Capital Market Supervision, ILITA guidelines, Government ICT Authority directives and others. When making this comparison, it is necessary to examine all active applications in the cloud in the organization. This mapping can be done, inter alia, by examining the users' browsing history and comparing it with the software providers list by examining existing rules in the relevant communication components (such as firewall, filtering, etc.). In many cases software for payroll management, document sharing, forms building and surveys and more are in the cloud, and the organization is 'unaware' of that (Shadow IT).	2



Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Public cloud computing:	11.4	Define and implement processes for periodic supervision and control of the provider's compliance with its obligations. 	Cyber protection application in cloud services based on the service provider' strict fulfillment of its obligations. It is necessary to take supervision measures in order to ensure that the provider fulfills these, either by direct supervision or by an independent third party which reviews periodically the provider's compliance with its obligations.	For example: sending questionnaires to the provider, auditing the provider, using external and objective Review services, indicating the provider's compliance with its obligations. The service. software provider will send to the client. detailed record of its compliance with the requirements defined in the agreement, and their implementation.. provider's deviations from the agreement have to be approved by the director of Cyber-Defense in the organization. For example, in case of. fundamental requirement by the organization for compliance with specific SLA policies, or. password policy that the provider cannot perform,. formal procedure is required, whereby the provider explains why it cannot meet that requirement and whether it expects to close this gap. These data will be transferred to the director of Cyber-Defense in the organization for approval and for defining compensating controls to reduce the risk.	2
Public cloud computing:	11.5	It is necessary to carry out independent information security checks of interfaces to cloud services that are exposed to the Internet.	Testing of cloud services by the organization. by. third party hired for this purpose, or by some other objective party. makes it possible to identify information security exposures and handle them without having to rely exclusively on the provider.	The relevant tests can include: testing of penetration of user interfaces, management interfaces and applicative interfaces, audits in accordance with generally accepted standards, or audits covering specific topics defined in the contract with the provider.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Public cloud computing:	11.6	<p>Make sure that no data, which under the regulation and responsibilities of the organization must not be transferred, is transferred to the cloud services.</p> 	<p>There is data that the organization is prevented from transferring for storage or processing in public cloud services due to regulatory considerations or Commitment to third parties. Prior to transferring data to the cloud make sure that such data are not kept or transferred to the cloud services.</p>	<p>For example, an examination of the data fields that the organization plans to transfer to the cloud services before making. decision on the matter. Can also perform by deletion or substitution of such data in the records transferred to the cloud services.</p> <p>Consultation with. qualified legal entity when performing an examination and evaluation of the sensitivity of the data and the possibility of transferring it for storage in the cloud.</p>	1
Public cloud computing:	11.7	<p>The business continuity plan of the organization is required to take into account situations of revocation of the ability to access cloud services.</p>	<p>Cloud services are external to the organization, and connection to them is usually through public infrastructure, such as the Internet. It is necessary to consider, as part of the business continuity plan, situations where there is no access to the cloud. whether due to. malfunction at the provider, or because of. failure in the infrastructure of accessing the provider.</p>	<p>For example, alternative methods for providing services to customers in the event of disconnection of cloud services, updated data files in the organization, containing information that exists in the cloud services.</p>	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Public cloud computing:	11.8	Set up and implement mechanisms for access control, suitable for access interfaces to cloud services, in accordance with the threats and exposures relevant to each interface.	Cloud services typically have several types of interfaces: user interfaces, management interfaces and maintenance and applicative interfaces. Generally, these interfaces are exposed to the Internet and public networks, and therefore it is imperative to set strong access control mechanisms, appropriate to the nature of the threats relevant to the interface, to the technological exposure level of and the outline of the threats.	For example, strong authentication management interface, limiting access to sensitive interfaces to certain Internet addresses.	2
Public cloud computing:	11.9	Ensure that the cloud service provider implements secure development processes and integrates information security testing in the development and maintenance stages.	The main exposure areas of 'software as a service' (SaaS) in the cloud are user and application interfaces. In order to reduce such exposures, the cloud service provider must implement secure development processes and integrate appropriate security checks during development and maintenance stages. The organization must ensure that the provider properly implements these processes.	For example, the provider's declaration that it is implementing secure development processes, presentation of results of periodic information security tests performed on the provider's systems.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Public cloud computing:	11.10	Ensure that the cloud service provider implements mechanisms for information security monitoring and reports to the organization regarding exceptional events.	There are areas in the field of Cyber-Defense, which are under the responsibility of the cloud service provider. The organization should ensure that the provider performs monitoring of these areas and reports to the organization (the service's client) regarding suspected cyber-incidents, in order that the organization could take protective actions at his side: containment and recovery.	Can be applied through the inclusion of the issue in the contract with the provider and periodic reporting by the provider on the number of events that have occurred and their analysis.	2
Public cloud computing:	11.11	There must be mechanism for monitoring security events in order to detect cyber-events in the cloud services.	In order to get complete picture of cyber-incidents and suspicious events, the organization must monitor cloud service activities. This monitoring can be carried out using the cloud service provider's systems or by connecting the organization's monitoring systems to the log records produced by the cloud service provider's systems.	Can be realized by receiving events feed from the provider's system to the monitoring systems of the organization, or by accessing the provider's monitoring interfaces.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Public cloud computing:	11.12	Define and implement. mechanism that allows full functional continuity and deletion of data stored by the cloud service provider in case of termination of the service agreement with the provider.	Upon termination of the contract with the cloud service provider, the organization must enable functional continuity and retention of the records belonging to it, which have been preserved or processed using cloud services. In addition, ensure deletion of data that has remained at the provider and is owned by or under the responsibility of the organization.	Can be realized through the inclusion of this issue in the contract with the provider.	2
<p>12. Industrial Controls: Industrial control Systems (ICS) are responsible for controlling assembly lines, healthcare systems, electrical systems, building management systems (elevators, escalators, etc.), water infrastructure, etc. Due to the simplicity of these components, it was customary in the past to exclude them from the systems that the organization protects from cyber threats. However, these components are. favorite target for attackers, because damaging them could lead to serious damage to the organization and its customers. Accordingly, the organization is required to attribute high importance to the protection of these components and take special care to separate and isolate them from communication networks as much as possible. For this purpose, it is required to set. corporate policy regarding the controls, to protect their communications, manage physical access, the authorized personnel and the operations that may be performed (software updates, connect removable media, etc.) and implement mechanisms that monitor interference in their activities through. cyber attack. These controls are also suitable for embedded systems (OT) in general.</p>					
Industrial Controls	12.1	Write down, manage and monitor the corporate policy for the protection of the industrial control system environment.		Can be realized by writing policies and supporting procedures that define unique requirements for the industrial control system environment with respect to the nature of the controls' environment (Manufacturing, Logistics, environmental control, power production, etc.). Reference should be made to regulatory aspects available for these environments (e.g. FDA, GXP, cyber Authority).	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Industrial Controls	12.2	Defined rules for proper use of equipment in the production environment and place signage explaining these rules.	The organization will define. signage explaining the data security practices at the work stations governing and monitoring the production environment.	The signage may include the use of shared workstations, the use of removable media devices, users log off and more.	1
Industrial Controls	12.3	Define the sensitive processes where industrial control environments exist according to their degree of sensitivity.	The organization will map the processes where control environments exist and define the main business processes involving these controls in order to understand the level of business and regulatory damage that could result from such environments.	Document mapping processes and environments according to severity.	2
Industrial Controls	12.4	Separate control networks from other systems and external networks.	The organization will set apart control networks, users' networks or servers into separate networks so as to restrict direct access between networks	The separation can be carried out using firewalls and separate VLANs for every monitoring network. Given the option, it is preferable to separate by. one-way diode and allow only the release of information out of the organization.	1
Industrial Controls	12.5	Separate the management system of industrial equipment controllers and the operative components of the system.	Implement adequate separation between the operational controls network and the management system of the controls.		2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Industrial Controls	12.6	Do not connect devices that are not production environment controls to the production controls network.	The organization will not install equipment that is not part of the Industrial Control System in the controls network. Equipment which is required to be connected will be connected to separate network, and communication will be enabled individually.	If necessary to connect different equipment for interfaces with production systems, it must be connected by separate network segment behind the firewall.	1
Industrial Controls	12.7	Support providers access to the production network will be possible with prior authorization as well as by using secure and identified communication, which allows recording the provider's actions.	The organization will implement secure communications network for suppliers' access and will review the supplier's access to the organization by providing pre-authorization for any provider connection to the control network.	Can be applied using VPN server management system for dedicated users for each will provider (user priority for every employee of the provider), which will be usually locked and open only when necessary.	2
Industrial Controls	12.8	No direct access from the industrial controls environment to the Internet is allowed, neither from the human-machine interfaces environment.		It is possible to limit the control networks in the firewall and disable direct communication access from these networks to the internet. Updates will be allowed from buffer network individually, only after passing through equipment such as proxy.	2
Industrial Controls	12.9	Unnecessary services will be limited in the production environment and support systems, such as human-machine interfaces and smart sensors.	The organization will cancel and/or limit unnecessary services for all systems in the control environment, whether at the level of operating system, communications level and application level.	It is possible to be based on the manufacturers toughening documents of the operating system and applications, and shut down services, block ports, limit applicative access to certain functions and more.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Industrial Controls	12.10	Use reliable communication between industrial controls and terminal equipment if possible.	Use protocols that allow the source and destination authentication and encryption of the medium supporting the equipment.	In the event that it is possible to use secure versions of these protocols, use these versions (SFTP, HTTPS, SNMPv3 and others).	2
Industrial Controls	12.11	Set. unidirectional communication equipment from manufacturing to the sensory systems.		Set up tools for unidirectional communication transfer between sensors and systems in sensitive environments.	4
Industrial Controls	12.12	Wireless networks in the production environment will be separate from enterprise wireless networks.	The organization will implement. dedicated wireless network separate from the enterprise wireless network, to be used solely for control network communications. This network will not redirect to the enterprise network and vice versa.	It is preferable to avoid using. wireless network in the control networks, but if necessary for business. this network will be set up separately, and its management will be also separate and it will not be linked to any VLAN's internal network.	1
Industrial Controls	12.13	Wireless communication in the production environment will be limited by using secure protocols.		Use WPA-2 PSK, and if possible, it is recommended to use. digitally certified version for these wireless networks.	1
Industrial Controls	12.14	A separate user will be defined for each end client using. wireless network in the production environment.	The organization will set up. separate user for everyone and every wireless network equipment.	It is recommended to connect the wireless network to. dedicated Radius server, which will authenticate users of this network and enable their management.	2
Industrial Controls	12.15	Access to human-machine interfaces will be allowed through personal users for each operator.	The organization will define. personal user to anyone who works with the human-machine interface. If the position is shared, it is possible to use smart card identification.		2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Industrial Controls	12.16	Access to human-machine interfaces will be allowed by using strong authentication.	The organization will define strong authentication in accessing human-machine interface.	It is possible to use. variety of means, such as biometrics, smart cards, OTP and more.	4
Industrial Controls	12.17	Monitoring systems will be installed and activity recording will be carried out on the management servers.	The organization will set up. system for the recording. registration of activity logs on the management servers of the control environment.	It is possible to use. variety of means, such as tools for recording user screens and activities, recording of application logs, etc..	2
Industrial Controls	12.18	Install utilities such as intrusion detection tools in the management networks' environment of the production environment.		Can be realized by using Network IPS, HIPS tool and similar tools, such as Honeypots.	3
Industrial Controls	12.19	Install tools for file signature verification (Integrity Checking) to scan files being transferred to the management environment or installed in the management environment.		Can be realized using. variety of File Integrity Checking tools.	3
Industrial Controls	12.20	Install dedicated anti-malware tools in human-machine interfaces.		Can be implemented using anti-malware dedicated tools, depending on the type of system.	1
Industrial Controls	12.21	Manufacturer's software updates will be installed on the lower environments (test environments) prior to their being installed in the production environment.	The organization will ensure the installation of updates in. test environment and will run them over time in order to test the stability of the system and the process.	Can be realized by establishing. lower environment (at least partially), diverting communication to this environment during. maintenance window in the production environment and testing the process.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Industrial Controls	12.22	Install operating system updates that are supported by the provider in the production environment.	The organization will implement within. reasonable time operating system and application updates as received from the system vendor and will demand from the vendor security updates for serious flaws as they are published.		1
Industrial Controls	12.23	'Lock Configuration' tools will be installed on End Of Life systems, including obsolete operating systems.	The organization will implement tools that lock the system configuration in. 'clean' configuration if there is no option to update the equipment.		3
Industrial Controls	12.24	The ability to connect removable media to production equipment, including controllers, human-machine interfaces and sensors will be limited.		Can be realized by physically eliminating the USB devices (Fort Lock), or logically by operating system policy. GPO.	2
Industrial Controls	12.25	Removable media file transfer to the production systems will be carried out after 'laundering' the transmitted files.	The organization will implement. system of files 'laundering' and testing them thoroughly using some tools prior to transferring them to the controls environment.	Can be realized through the acquisition of. specialized laundering station, or, alternatively, by establishing. dedicated station, which includes several different scan engines.	2
Industrial Controls	12.26	There will be. redundancy system for critical components in the production environment.	The organization will implement. redundancy system of servers and critical sensors in the control environment for the purpose of process continuity.	In order to build redundancy it is recommended to consult with the control system vendor.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Industrial Controls	12.27	Physical access will be limited for business needs only to the industrial controls environment as well as to communications equipment in this environment.	The organization will limit physical access to the communication racks, hubs and management stations of the controls' environment	Can be realized by converting dedicated rooms to concentrated communications and servers, and perform access control using access tags. Biometrics for this environment.	2
Industrial Controls	12.28	Logical access will be limited for business needs only to the industrial controls environment as well as to communications equipment in this environment.	The organization will limit the access of corporate users who have no business relevance to the control system and will prevent their access to these networks and equipment.		2
Industrial Controls	12.29	Logical access will be limited, to the extent possible, (functional) to the production systems, including control interfaces, sample interfaces and human-machine interfaces.	Access to the management systems will be limited according to user profiles.. system controller will not change settings and parameters of. system. Changing the parameters will be carried out by an administrative user.	It is possible to verify with the system's manufacturer whether the system can use different user profiles.	3
Industrial Controls	12.30	Carry out information security testing in the production and management environments and interface, including penetration tests.	The organization will define. comprehensive tests outline for tests including the variety of control network components, with an emphasis on comprehensive information security tests for all components, in order to maintain the continuity of the business process.	Can be realized by checking the configuration of the environment, running simulations during downtime windows and performing penetration tests in these networks if possible and. or during maintenance operations.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Industrial Controls	12.31	Set up unique monitoring scenarios in the production environment and monitor them through an organizational monitoring array.	The organization will define. range of dedicated monitoring scenarios for the control environment in accordance with the threat outline and the importance of the system to the business process.	Network monitoring in control networks is different from ordinary systems monitoring since the sensitivity threshold is lower. Any deviation from the amount of normal communication between the controls and the management interfaces and sensors may indicate. potential cyber-incident, since the activity in these environments is continuous and monotonous.	2
<p>13. Securing Mobile Phones</p> <p>Cell phones have become major professional tools. they contain the contacts, email correspondence, various enterprise applications, passwords and more. In many cases they allow access to corporate networks and web browsing. Hence,. correct definition of phone privileges, of their business use and their protection is critical to the organization's Cyber-Defense. It is necessary to set for them access control, configuration security, implementation of dedicated protection tools, securing communication channels with the organization, centralized management. including remote control in case of loss, and more.</p>					
Securing Mobile Phones	13.1	Set up mobile phone usage policy and update it periodically.	The organization must set up. mobile phone usage policy according to its needs, including access to enterprise applications and maintaining the organization's sensitive data on the mobile phone.		2
Securing Mobile Phones	13.2	Implement protection mechanisms for controlling access to mobile phones, such as passwords or biometric measures.	The organization must set the parameters for controlling access to mobile devices, such as. password of. certain length and automatic locking.	Can be realized using automated policy settings, applied on the device when connected to. network organization.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing Mobile Phones	13.3	Implement security settings on phones, that restrict access to mobile phone, keep software up to date, limit risks of installing dangerous apps and so on.	The organization must set various parameters for implementation in the operating systems of mobile phones and enforce implementation of these settings on the devices. These settings include enforcement of software updates, restricting hazardous services, limiting installing unknown or risky software and so forth.	Can be realized using automated policy settings, applied on the device when connected to the enterprise network or through centralized management system.	3
Securing Mobile Phones	13.4	Implement encryption of sensitive data stored on mobile devices.	The organization's sensitive data, stored on the mobile device, such as corporate email, sensitive files and sensitive applications, will be encrypted using the device's operating system or through dedicated applications.	Settings can be applied using applications which perform data encryption (Secure Email application, for example), or by means of encrypted partitions using the operating system.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing Mobile Phones	13.5	Implement dedicated protection tools that detect and block unauthorized access and hostile applications on mobile devices.	Mobile devices, especially those owned by employees of the organization, are particularly exposed to the infiltration of hostile programs, whether inserted into device without the knowledge of its owner or disguised as an innocent application. In order to prevent malicious code that could expose sensitive enterprise information, run specialized applications that detect and prevent the running of hostile code.	Can be applied using commercial systems designed for protecting mobile devices, or using commercial devices that implement this type of defense capabilities.	3
Securing Mobile Phones	13.6	Implement encryption of sensitive data in inbound and outbound communication of mobile devices.	Data communications, inbound and outbound from mobile phones, makes use of unsecured public networks. In order to protect the information from exposure. it is necessary to encrypt it.	Can be realized using conventional encryption protocols and using applications which perform encryption operations while accessing the organization's network.	2
Securing Mobile Phones	13.7	Implement access control measures on the organization's mobile network.	Mobile devices that connect to the corporate network are using remote access interfaces to the network. In order to secure this interface, access control must be implemented, such as the use of digital certificates technologies and passwords.		3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing Mobile Phones	13.8	Implement. centralized management system, which manages the configuration of mobile devices and enables remote deletion of data from the device.	The enforcement of secure configuration of mobile phones and the remote control of sensitive data stored on mobile devices is made possible through. central management system and management components, which are applied to the devices.		2
Securing Mobile Phones	13.9	Implemented. central information security monitoring system, which receives alerts on unusual events on mobile devices and enables containment and response to incidents.	In order to detect attack incidents on mobile devices and enable their containment an. suitable response, it is necessary to implement. centralized monitoring system, which receives alerts from components applied to the mobile devices.		3
Securing Mobile Phones	13.10	Set. policy for the protection or restriction of calls made through mobile phones.	Mobile devices use unsecured public networks. the organization must set etiquette and caution rules when making phone sensitive calls.		4
<p>14. Change Management: The organization's cyber environment also needs to make changes and periodic updates, being part of the organization's development and update process. These include the acquisition of companies and integrating them within the organization's infrastructure, technological upgrades, addition or changing business processes (e.g. Supply chain), and more. These changes or updates Processes entail. great risk of harm to the systems of the organization and the information in them. Accordingly, the organization must manage the changes so that they will reduce the risk. This management includes. configuration management policy for the cyber environment in the organization, its documentation and ongoing updating.</p>					
Change Management	14.4	Write down and implement. configuration management policy, Review and update it periodically.		The chapter of Change Management is in the corporate information security policy and supporting procedures.	2

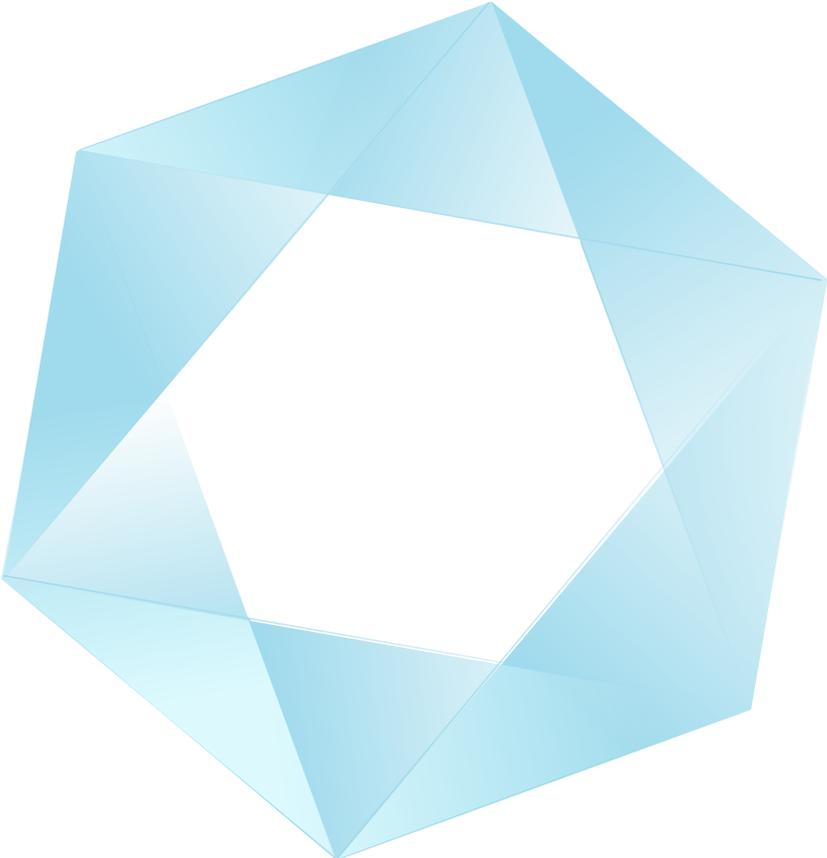
Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Change Management	14.2	Set up, record and update when necessary the required basic configuration of the information system.	The organization will record the information system configuration during its establishment, including documentation of components, communication, system settings, as well as its installation procedure.	Can be applied by preparing system portfolio.	2
Change Management	14.3	Examine the existing configuration of the information systems on a periodic basis and when events occur, which were defined by the organization and are an integral part of the process of installing and updating version.	The organization will record the changes in the information systems during major reconfiguration, or once every period (whichever comes first).	Can be realized through process of documenting changes.	2
Change Management	14.4	It is necessary to implement automatic mechanisms in order to keep the basic configuration of the information system up to date, including its integrity and preparedness of the settings.	The organization will implement backup and restore set for the configuration of the information system and its components.		3
Change Management	14.5	Keep previous versions of the system configuration to support Rollback.	The organization will ensure that there are tools and methods for rollback for unsuccessful changes.	Can be applied using full system backup before the change and through gradual upgrading of components (testing environment, DR environment, etc.).	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Change Management	14.6	Determine which changes to the system are defined as configuration changes, document configuration change requests and their status (approved, executed, rejected) and keep them for a defined period of time.	The organization will manage the process of ratification of changes before applying them.	Can be applied through holding weekly change management meetings and ratifying changes while explaining the nature of the change.	2
Change Management	14.7	Implement an automatic mechanism for documenting requests for configuration changes, for alerting the certifying authority and to prohibition against making changes until receipt of all necessary approvals.	The organization will operate an information system which will coordinate the change management process in general and the changes ratification process in particular.		4
Change Management	14.8	Analyze changes in the information system in order to determine potential security effects before implementing the change (due to the weakness, lack of compliance, malice, etc.).	The organization will manage the risk assessment process as part of the organizational change management. Potential impacts on system availability and reliability will be documented, as part of the stages of submitting an application for changes.	Can be applied via a supplementary questionnaire for management changes request, which will list its risks when carrying out the changes.	2
Change Management	14.9	Analyze configuration changes in the information environment in a separate test environment prior to its implementation in the production environment.	The organization will examine the changes in a separate test environment before implementing changes in the production environment.	Can be realized through maintaining a test environment, in a version resembling the production environment.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Change Management	14.10	After carrying out configuration changes in the information system, check the security functions in order to make sure that they work properly.	The organization will check the entire system and its components with respect to the information security aspects, including: authentication, authorization, encryption, toughening and any other information security functionality in the system.	It is necessary to execute, through the required monitoring overview and, if necessary, even through tests such as controls survey and penetration tests.	3

15. Media Security

Media (magnetic, removable, optical, mechanical) are used for entering and extracting information from the organization. Media used for storage and portability of information both within the organization and outside it. This information may be sensitive for the organization, its customers or its suppliers, and therefore it is necessary to protect it from getting into the hands of any unauthorized factor. Media may also be used to insert abusive software within the organization. Therefore, it is necessary to define and implement. policy of handling and protection of media (including media scrapping).



Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Media Security	15.1	Write down and implement. media protection policy (magnetic, removable, optical, mechanical), Review and update it periodically.	The organization will write and implement. usage and protection policy for media, including reference to the use of the media, the manner of its storage and the destruction of the information stored on this media and. or the destruction of the media itself at the end of use (or the end of life of the media).	The policy will consider, for example, the types of approved devices against those prohibited to make use of, whether use of the media is allowed or prohibited (such as. computer. portable memory, work phone) for private purposes, is it permitted go out with this media outside the organization, and how, what to do with the media when it is faulty. deprecated. From this policy will stem the relevant procedures for the organization, such media mapping processes and distributing media (such as purchasing magnetic discs for the servers, optical media) and providing access to the aforementioned media in accordance with the organization's procedures for the relevant officials (such as access to hard disks only to IT personnel, access to removable media for the relevant officials, etc.).	2
Media Security	15.2	Label each media according to the security level of the data stored, noting its treatment in relation to data security and distribution limitations aspects.	The organization will define labeling procedures and processes of the media, as well as label the media according the security level of the data stored.	The media can be labeled with stickers glued to backup tapes, outgoing packages of hard disks, and optical disks.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Media Security	15.3	Store media securely.	The organization will define data storing security methods, according to various media types (magnetic, optical, removable).	Can be implemented by physical protection of physical media storing areas, backup encoding and storing magnetic media at. licensed storing facility; protecting communication cabinets containing servers, storing devices and hard disks; storing optical media and storing components of encoding devices (HSM), in strongboxes.	2
Media Security	15.4	Define media blackening and/or destruction processes.	The organization will define procedures and processes for the blackening (Blackening. deleting all sensitive data from. component, prior to its exiting the organization or assignment to. different use) and destruction of media, as well as conducting. continuous surveillance of the implementation of these blackening and destruction procedures. Ensuring that sensitive data does not exit the organization without control.	Blackening of media can be performed manually (such as individual deletion of sensitive data: credit card details, details which may serve to identify clients, etc.), or technologically (systematic deletion of pre-known patterns). Media destruction can be done by shredding/magnetizing/ resetting by overwriting.	2
Media Security	15.5	While connecting removable media to the organization's network, clean it, to ensure that the media do not contain malware or other malicious components.	The organization will define. data whitening process (scanning for and cleaning malicious code threats), before incorporating the media within the organization's systems	Can be implemented by defining special whitening stations, to scan the media before its connection to the organization's systems.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Media Security	15.6	Define and implement media use limitations, using security means	The organization will define and implement media use limitations technologies and methods. In order to minimize data leakage from or malicious code penetration threats to the organization's network, via removable media.	Can be implemented by toughening workstations according to the system/station type, or the employee's authorizations, allowing only authorized employees to connect removable memory devices (such as. Disk On Key) to the computer. On may implement. definition by which any data stored from. station on. removable device will be encrypted.	2
Media Security	15.7	Implement encryption mechanism to secure digital media transferred outside the organization. 	The organization will implement encryption technologies regarding media intended to exit the organization, or is in constant use outside the organization (removable media)	Can be implemented by removable data encryption tools, encryption of backup tapes, during backup, etc.	3
Media Security	15.8	Periodically inspect the media whitening and destruction equipment, to validate its effectiveness.	The organization will define an inspection process of media whitening and destruction equipment, including checking the effectiveness of the implemented processes and technologies.	Whitening/destruction systems can be inspected periodically by samples, such as trying to insert. "dummy" file, trying to read or retrieve. sensitive file from obsolete media.	3

16. Supply chain and Outsourcing:

Many organizations are dependent on services bought from external suppliers. These may be sub-contractors producing computerized components, suppliers of computing services, various applications bought from external suppliers, etc. Such services may be linked to the organizations' systems, therefore constitute potential attacking channels. Therefore, the organization has to defend itself against being damaged by its suppliers. It does it with legal and contractual demands from its suppliers, by surveying suppliers' Cyber-Defense mechanisms, by devising work procedures, etc.

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Supply chain and Outsourcing	16.1	Defend against supply chain threats on the system, as part of. Defense in Breadth	The organization will map and detect threats and risks stemming from suppliers' systems/services, technologies and processes, and map the risks as. part of the organizational risk/threat management.	The mapping process may be aided by. cyber intelligence collection about the supplier, in order to consider such information in considering and deciding on risk management. One should consider the supplier's existing mechanisms, controls and processes, and their influence on the business processes supported by the system/service. For example: automation controls and virtual servers installed by the supplier on. cloud platform, and their toughening method, may influence the organization if these environments are not toughened enough or the cloud services supplier is not secured/situated in. hostile country, etc.	2
Supply chain and Outsourcing	16.2	Use legal and contractual tools when purchasing. data system or. service from external suppliers 	The organization will use contractual mechanisms, such as limited liability and other legal mechanisms, to minimize the risks emanating from the purchase.	In addition to limited liability and indemnity clauses, compliance with regulatory and legal requirements, one may stipulate clauses such as early alerts, in service or expanded support interruption beyond the system's End-Of-Life, confidentiality agreements, and secure data storage, or any other clause constituting. control factor, compensating for the risks embedded in establishing the system/purchasing the service.	2
Supply chain and Outsourcing	16.3	Perform. supplier survey prior to signing. services/ products purchase contract	The organization will survey the suppliers character and conduct, prior to signing the contract	The supplier survey may examine: the supplier's maturity, integration. customer number, stability, service capability, data security mechanism, business continuity, etc.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Supply chain and Outsourcing	16.4	In cases of connection to the supplier's network, one should implement preventive controls, in order to minimize damages caused by the supplier's infrastructures.	The organization will use its own or other designated controls in order to minimize damages caused by the supplier's infrastructures.	Such controls can be environment/interface separation, sanitation of the supplier's output, separating communication by proxy server, etc.	3
Supply chain and Outsourcing	16.5	Before installation, inspect the data security aspect of the system/service.	The organization will inspect the system/service with its own tools, as well as by trying to penetrate it before moving into production.	The system can be examined either by vulnerability management tools or by risk surveys and penetration tests, to insure the non-existence of dire findings which may damage the organization and its processes.	4
Supply chain and Outsourcing	16.6	Define the importance level of the system/service in relation to depended business processes	The organization will define. certain system as critical if any damage it suffers influences. critical business process.	Add the system/service to the critical systems list. Monitor it to verify its continuity.	3
<p>17. Securing purchase and development</p> <p>In purchasing and development processes the organization introduces cyber components into its systems (purchasing. new software system, developing. specialized tool). Malware may penetrate the organization's network via purchasing and development processes. On the other hand, various defenses may be integrated during product's development, which will assist the organization in the future to cope with cyber threats. The controls are intended to minimize the risks that. purchase or. system/software developed will introduce cyber risks into the organization. Controls include: defining. policy to direct all entities within the organization (purchase, legal, project managers, developers, etc.); defense requirements from purchase/development entities; risk management in purchase/development, defenses all along the software/system life cycle.</p>					
Securing purchase and development	17.1	Write, implement, and periodically review, purchase and development policy.	The controls are intended to verify that all systems comply with the security benchmark defined by the organization, both those developed in-house and those purchased from the shelf or as. cloud service.	This policy will include, inter alia, reference to the SLA level desired, complying with protection requirements at all levels (password policy, Logs, encryption etc.), remote access, developers access to production etc.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing purchase and development	17.2	For systems with. 3+ value level, ensure compliance with standards, by an external, independent, entities.	The organization will ensure that assets ranked in the value questionnaire,. 3 or above, comply with all requirements of the Defense Methodology. This shall be done by. surveyor external to the developing/ purchasing organization.	In cases of in-house development, one may be assisted by. counseling/ recording firm to examine compliance of the system protection with the Defense Methodology. In cases of external purchase, ensure that the system complies with the Methodology 's level. requirements, or, alternately, require the supplier to present certificates of compliance with common standards, such as SOC1/SOC2, as well as other requirements (such as compliance with PCI, HIPAA, etc. according with the type of data stored/processed by the system) these certificates will be stored and backed up in the purchasing/ development agreement (including. commitment to notify if the certificate is voided or expires.	4
Securing purchase and development	17.3	Cyber risk management. evaluate the cyber and data security risks involved in the development or purchase of. new system/ service. Manage them according the existing risk management processes.	The control in intended to verify that protection aspects are considered from the initiation and planning through the development and production phases. Ensure that initiation, purchase or development follow. survey of the risks involved, and their integration within the organizational risk management.	It is recommended to carry out the initial risk management in the initiation phase, so as to be prepared to integrate controls within the development process, or ready to live with the detected risks. One may be assisted in risk management with known methods, such as SSDLC, SANS/OWASP publications. Take note to outsourcing and cloud systems, they incorporate specific risks, some of which are described in this document. It is recommended to become familiar with the recommendations of specific standards: ISO 27017, CSA etc.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing purchase and development	17.4	<p>Cyber protection as part of the development life cycle. it is necessary to take into account security considerations at each stage in the life cycle of system development and define officials for security aspects at every stage.</p> 	<p>The organization will promote an orderly process of secure development, defining the stages of implementation of information security at every stage in the development process and make sure that the key factors responsible for various stages in the development process accept responsibility for their roles on the issue of the developed system's security and are equipped with the necessary knowledge to do so.</p>	<p>It is possible to define information security requirements at the initiation phase, at the design phase (the POC phase), at the implementation phase (procurement, development and implementation phase) and at the submission stage (information security testing and trials before going to production). At these stages it is necessary to define the guidelines and responsibility to make sure that the security considerations and requirements in the process are met. Security considerations in the project will also include aspects that are not technological, or that do not relate directly to the development and submission, such as storing information at the supplier at the end of development, compartmentalization at the suppliers' premises, remote access procedures, SLA, commitment to support the product for. specified period, the method of transferring files and information of the customer to the supplier, etc. Use the controls included in the Outsourcing chapter herein.</p>	

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing purchase and development	17.5	Include the following requirements and criteria for closing the purchase contract of the system. component. service: functional security requirements, requirements for protection, monitoring requirements, documentation requirements, setting up. production environment, admission requirements.	The goal is. formal definition of protection requirements for each project and contracting at the contractual level.	It is possible to define. templates collection of documents of information security requirements to use when characterizing systems in development. procurement. The document will include the controls expected from the vendor to be addressed in accordance with the expected values level of the planned system according to the criteria of the Defense Methodology.	
Securing purchase and development	17.6	The system's developers should be required to supply. functional description of the security controls to be implemented, and information regarding the design and implementation of these controls.	The organization will demand full documentation of the data security controls integrated within the system, to ensure compliance with the data security requirements, and for the sake of the organizational risks and threats management process.	It is recommended to get hold of the functional, high, and low levels design documents (FD, HLD, DD/LLD), including controls documentation, as part of the system's full documentation. Such documentation will include, inter alia, the encryption type, the input tests, the Cyber-Defense scripts, etc. as. part of the documentation, the supplier will refer to its own development and to external applications (libraries, plugins, third party software, external interfaces, etc.). This control is not intended to verify the mere implementation of security requirements, but its manner (protocols, processes, supporting tools, etc.).	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing purchase and development		Secure Architecture. implement secure architecture principles within the characterization, design, development, implementation, and alteration of. data system.	The organization will ensure that secure architecture is implemented in system planning, whether in-house, or while controlling an external supplier processes.	Secure architecture principles can be derived from controls described in the present document, from common standards, etc.	2
Securing purchase and development	17.7	Secure architecture. implement secure architectural principles in. framework of specification, design, development, realization and change in the information system.	The organization will ensure that when designing systems and services. secure architecture is implemented, whether planning is carried out, coordinated or supervised by the organization, or through the control of the organization of the work of the external supplier.	Secure architecture principles can be derived from controls cited in sections of this document, and other accepted standards.	
Securing purchase and development	17.8	Secure development. require system developers to employ secure development tools and methods, as an integral part of the development process.	The organization will integrate secure development methodologies, and ensure their assimilation within systems and services suppliers performing developing processes.	A software supplier will deliver documentation of its actual implementation of secure development principles, detailing the tools and methods used, the controls to be supplied for the system's protection level, etc.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing purchase and development	17.9	Secure operation. maintain. data system management manual, including the best security configuration method.	The installation and operation manual, will include the information necessary for. secure configuration.	Within the configuration documentation include: an installation manual, infrastructure and application toughening, recommended deployment, etc. For. and above value level systems, pre-affirm the recommended system configuration, such as open ports, network use, employing verified protocols, default password changing, etc. since configuration change management is hard to control and follow manually, assets of value level. and above will include. compensation mechanism for automatic configuration changes testing (rules within the SIEM,. central configuration management system, Continuity control monitoring).	2
Securing purchase and development	17.10	Securing the supply chain. its demand suppliers to comply with the organizational security requirements, to regulations, standards and directions.	The organization will ensure that its suppliers comply with its directives, as well as with the regulations of the states where it is active.	The organization's regulatory requirements can be defined as part of. standard data security requirements screen, designated to all external service suppliers.	1
Securing purchase and development	17.11	Data security testing and correction should be performed before integrating systems and services. Such tests will include, at least, functionality testing (compliance with requirements) and security exposure.	The organization will ensure that security tests were performed before. new system or service are operational, and following each update.	In cases of services supplied by external suppliers, one may rely of tests performed by or for the supplier.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing purchase and development	17.12	Document the data security flaws and vulnerabilities correction process.	The documentation is intended to ensure the integrity and effectiveness of the process.	The control is intended to verify that flows are treated according to the organization's policy. This tracking will locate long standing grave flows, unsolved companywide flows, will assist the Cyber-Defense manager in devising periodic work plans, and will be presented to the management periodically.	2
Securing purchase and development	17.13	Perform. Static Code Analysis as. part of data security test of. new system/service	The organization will test level. systems with automatic tools replacing manual surveys (Code Review)	Code analysis can be performed by automatic tools, testing various code configurations (source code, compiled, URL etc.) thus identifying loopholes. Perform code analysis before purchasing. system and following any changes to its environment.	3
Securing purchase and development	17.14	Validate system risk and vulnerability evaluation following the completion of its development.	The risk evaluation validation is intended to ensure that the risk evaluation performed in the analysis Stage is matching that of the developed system.	Perform. risk survey following the completion of development and prior to production	3
Securing purchase and development	17.15	Data security tests should be performed by an external, independent, entity.	The organization will define the scope of the survey to be performed by the supplier, and its type (white/ gray/ black hat). The survey will be performed by an external, independent, entity.	Conducting. PT in-house may give rise to conflict of interests within the organization. Employing an external entity will improve product defense. In using automatic tools,. third party can validate that the tool is performing penetration tests covering the system's scope. The same party will make the outputs accessible to the organization (writing the final report). Testing will be carried in an environment similar as possible to production.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing purchase and development	17.16	Perform penetration testing to the system/ service.	The purpose of control is to examine the effectiveness of the controls and protections in practice. This is accomplished through challenging and attempts to penetrate the system. infrastructure.	These tests can be carried out by applying automatic assault tools or through human factor. These tests may include attempts to get unauthorized access, introduce malicious code to the database and implement well-known attacks, such as SQLI, XSS, CSRF etc.	3
Securing purchase and development	17.17	Verify that the system tests include verification; that defined data security controls are implemented according to the original design.	Maintain. tagging list of defense requirements defined to the system, and verify that all requirements are actually fulfilled in-house and by the supplier.	At the delivery phase, verify that all requirements defined in the LLD, are actually implemented. Document the test nature and outcomes.	3
Securing purchase and development	17.18	Require the supplier to perform Dynamic Code Analysis of. new system/service	Require the supplier to perform Dynamic Code Analysis of. new system/service	Dynamic Code Analysis will be performed by existing, off the shelf, tools or by Fuzzing, as well as by automatic scanning tool during. system run. The organization will inspect periodically sample reports or findings, to verify correction of flows accordingly.	3
Securing purchase and development	17.19	Implement. tamper resistance mechanism within the system.	The organization will verify that the developers implemented within the system. tamper resistance capability.	Tamper resistance mechanisms can be implemented by digital signatures, encryption, creating copies, etc.	4
Securing purchase and development	17.20	Implement methods to prevent intrusion of false system components	Such mechanisms are intended to prevent the intrusion of false software of hardware components into the organization, intentionally or by misleading an element of the supply chain.	Such mechanisms may be: verifying software components, inspection and verification of incoming software files, etc. such mechanisms can consist of various security levels. from compartmentalization of physical access to computers, BIOD password, dusk encryption, limiting the operating system to BOOT from the HD only, rules within the SIEM system etc.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Securing purchase and development	17.21	Verify that purchased. developed systems implement input verification mechanisms.	Developed systems will implement unexpected inputs filtering mechanisms, such as unexpected lengths or formats. These may lead to unexpected outcomes, and have negative impact on the system's immunity, integrity, or availability, according to its value level.	Can be done for level. systems with. supplier declaration regarding input verification and the use of standard software libraries filtering inputs according to their expected characteristics. For level. systems. technological solution is required (such as WAF) at the network level, or. similar mechanism at the application level. In delimiting the penetration tests, verify that input tests are fully covered (OWASP can be. good reference point), and in accord with the organization's policy.	2
Securing purchase and development	17.22	Verify that purchased/ developed systems implement error management mechanisms.	Developed system will implement mechanisms to capture errors and to present system errors without exposing sensitive data. In any case verify that the error mechanism does not expose sensitive system data, such. table or user names, software language and versions, etc.	Can be done by implementing an error management mechanism, presenting standard errors.	2
Securing purchase and development	17.23	Verify that purchased/ developed systems implement output verification mechanisms.	Developed systems will implement mechanisms to filter unexpected outputs, which may result from an attack on the system, and expose sensitive data.	Can be implemented by using standard software libraries, that filter output according to its expected formats. Or by anomalies identification systems, based of the system/user/ operating system behavior, etc.	3
Securing purchase and development	17.24	Verify that developed/ purchased systems implement session reliability mechanisms	Developed systems will implement mechanisms intended to prevent session hijacking, man-in-the-middle etc.	Can. done by proper session management, deleting connections at the end of users' activities, tokens randomness, etc.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
18. physical and environmental protection:					
Physical and environmental protection is an important Cyber-Defense layer of the organization, intended to block physical penetration of the cyber environment. Preventive activities include, inter alia: allowing physical access to the organization's installations to authorized persons only; physical protection of the cyber infrastructures: electricity, air-conditioning; water damages, etc. in addition, an effective physical protection prevents malicious damaging of equipment, as well as notifying the authorities in such attempts. This chapter covers only physical protection of cyber components.					
Physical and environmental protection	18.1	Write, implement, and periodically control and update physical and environmental protection policy.	The control aims to define the organization's policy regarding locking doors at the end of the day, security cameras, visitors, and external employees' entry into the company's sites and sensitive areas, proper protection of server and control rooms, etc.		2
Physical and environmental protection	18.2	Write and implement procedures, to integrate. physical and environmental protection policy and relevant controls	Prepare site physical access control procedures, including: 1. Physical access procedure; 2. Guests procedure;. computer/ communication room access procedure.		2
Physical and environmental protection	18.3	Define and maintain. list of all persons authorized to enter the site containing the asset. Issue identification means to authorized persons, survey the list periodically, deleting persons whose access is no longer necessary.	Maintain and update the authorized persons list.	Issue employee/visitor card for identification	2
Physical and environmental protection	18.4	Enforce physical access control at the installation's entrance/exit points.	Enforce physical access control at all sites of the organization.	A door. card reader, lock, biometric reader,. guard, combination code, etc.	2
Physical and environmental protection	18.5	Maintain logs of physical access to the installation.	Record and store logs of all entries and exits of all visitors.	Store all entries and exits manually, by. guard, or in. database.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Physical and environmental protection	18.6	Control, record, secure and enforce physical access control to communication/ computing areas (server rooms/ communication cabinets). 	Limit physical access of unauthorized elements into communication/ computing areas (server rooms/ communication cabinets). The organization will define. list of authorized persons and enforce access according to its procedures.	Define physical and logical access permits for authorized persons. 2. Record by logs or log books all access to computer rooms. In cases where it is not possible to record access to communication cabinets and server rooms, consider physical protection by locks, preventing access to unauthorized persons.	2
Physical and environmental protection	18.7	Have physical control of the system output devices, in order to prevent unauthorized elements from acquiring the output (printers, fax machines, etc.)	The control insures that outputs reach their original owners. It is especially important for outputs containing personal information, such as medical or insurance data, private employees' details, etc. in such cases, ensure that the information reaches only those authorized to see it.	Can be achieved in several configurations: 1. By printing control system, requiring. code, or employee card to receive output; 2. Place printers in closed rooms with limited access. 3. It is possible to use fax2mail services, or at least ensure that the proper receiver is in the vicinity. fax machine, before. message is printed. 4. At the end of the day, insure that all output devices located publicly, are "clean" thus private information is not available to unauthorized persons.	3
Physical and environmental protection	18.8	Monitor the physical access to the installation containing the asset, in order to detect and respond security events, and to periodically survey activity logs.	This control is intended to block access of unauthorized elements to sensitive areas. An access potentially allowing them to act maliciously, such as installing listening devices, connecting to the network, stealing hardware, etc. Proper control means, that only persons authorized by the organization have access to these areas.	Monitor all physical entrances to sensitive areas, such as server rooms, communication cabinets, etc., by registering all entries and exits.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Physical and environmental protection	18.9	Monitor and raise alarm at any physical access to an asset out of normal working hours and days.	Use monitoring and alarm technologies in order to detect unauthorized access attempts out of normal working hours and days.	Use alarm systems/security company, to monitor and alarm from unauthorized accesses to the installation.	3
Physical and environmental protection	18.10	Define and maintain. response array to unauthorized accesses to the installation.		By an organizational security officer,, security company, etc.	3
Physical and environmental protection	18.11	Install. closed circuit television system, to monitor any physical access to the asset. Store the recordings for. pre-defined period.	Install. closed circuit television system, to monitor any physical access to the asset. Monitor the CCT continually by. security person.		4
Physical and environmental protection	18.12	Record all visitors to the installation	Record all visitors to the organization's installations	Maintain. visitors' log/ record, in. designated system all visitors to. specific installation.	2
Physical and environmental protection	18.13	Prevent damage from the system's electrical equipment and cables	Be punctilious in installing and tagging all electrical cables in the server rooms, and communication cabinets.	Tag all cable endings so that employees may easily detect their association with servers/systems, thus avoiding faulty disconnections.	2
Physical and environmental protection	18.14	The organization should be able to securely supply electricity for short periods, in order to enable an ordered shutdown of. system, or its transfer to an alternative power source		Install. UPS array, to secure an ordered shutdown of systems, in cases of power shortages.	2
Physical and environmental protection	18.15	The organization should be able to securely supply electricity for longer periods, in order to achieve. continuity of business activities		An electrical generator is. good option.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Physical and environmental protection	18.16	Implement and maintain an automatic emergency lighting system, including emergency exits and evacuation paths.			1
Physical and environmental protection	18.7	Implement and maintain fire extinguishing systems, specifically for data systems, supplied by an autonomous power source.			1
Physical and environmental protection	18.18	Maintain and monitor acceptable temperature and humidity level at the asset installation		Especially in server rooms.	2
Physical and environmental protection	18.19	Protect the asset from water leakage, by either. master shutoff or insulating valves			2
Physical and environmental protection	18.20	Verify and monitor system elements entering and exiting the installation		For example by. removal procedure of software/ hardware elements from the organization, especially those that may store sensitive data. Monitoring and controlling information exiting the organization can be done by following hardware which exited (Laptops delivered to suppliers, disks on key, etc.). Periodic registering and monitoring will include: who received hardware, for how long, for what purpose, estimated retrieval date.	2
Physical and environmental protection	18.21	Implement security controls in alternative work sites (such as DR), assessing their effectiveness.		The physical security level at an alternative site, such as the DR site, will be acceptable, and suitable to the data stored there. Control implementation will be anchored in the contract with the alternative site management, and reviewed periodically.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Physical and environmental protection	18.22	Place system elements where damage impact potential, and unauthorized access probability are minimal,	If possible, locate systems (server/ communication rooms) in the best protected location, in the building's center, away from external walls and water sources (including piping).		3
<p>19. Human Resources: The organization's employees are an important organizational protection layer. On the one hand, they may detect and warn against suspicious events in real time, on the other, they may constitute vulnerabilities, which may lead to cyber-events, either by mistake or by being misled by attackers. Therefore, in recruiting, the organization should double check potential employees in relation to the sensitivities of their functions, inform its employees about cyber threats, possible defenses and reporting. The organization will define conduct rules of employees in the external cyber space (social networks, exposing internal information in Cyberspace. etc.), which may harm its protection level. All security authorizations of employees quitting the organization must be canceled.</p>					
Human Resources and employees' awareness	19.1	Evaluate the sensitivity levels of various functions in the organization, and define proper sorting criteria in employee recruitment.	Define minimum requirements in recruitment, and higher requirements for sensitive functions.	Minimum requirements can include, for example, background tests, and data verification, confidentiality test or. lie detector test. It is recommended to devise. matrix defining various tests for specific functions. For example, non-existence of. criminal record, conducting security classification tests when necessary, confidentiality and lie detector tests, verification of data submitted by potential employees, credential issued by former employers, technical support employees are required to pass. computerized confidentiality test, those having higher authorizations (ADMIN) are required to undergo an external test, etc.	2
Human Resources and employees' awareness	19.2	Conduct background test in recruitment and promotion to higher sensitivity functions	Conduct background tests to candidates/ employee prior to authorizing access to data systems	Background tests may include: background data verification, questioning former employers, confidentiality/lie detector tests, economic background verification, security clearance, etc.	3

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Human Resources and employees' awareness	19.3	Sign up employees on their commitment to the organization's cyber requirements.	The employee will sign documents, attesting to his awareness of the fact that the organization's systems contain secret business data, which should not be disclosed without specific authorization in accordance with the organization's rules.	Can be implemented by signing up all employees on non-disclosure agreements, kept in their files; by an IdM system controlling information about users on computers, and enabling periodical ratification of each employee.	2
Human Resources and employees' awareness	19.4	The organization will sign up all employees on non-disclosure agreements beyond their employment	Each employee will sign. non-disclosure agreement, and declare that no documents or other data storing devices containing business data are in his possession.	Can be implemented by signing up employees on NDAs, and by conducting tests on sample employees. Such reviews can be performed by monitoring users' activities on the network to locate anomalies (trying to access files unauthorized files, to copy large data amounts, etc.)	2
Human Resources and employees' awareness	19.5	Define security requirement of suppliers and third parties.	The organization will define data security requirements as part of its supplier relations policy. Such as limitations on data sharing, NDAs, instructing in the organization's security rules, suppliers' instruction, etc.	Can be implemented by rule booklet, and by signing up suppliers at the beginning of their employment. Conduct periodic refresher.	2
Human Resources and employees' awareness	19.6	Define regulations on using data systems at work. These rules define responsibilities and proper use of data systems, emphasizing sensitive systems.	The organization will define conduct rules in relation to data systems, distributing them among its employees.	Can be implemented by procedures defining download policy, surfing in data sharing sites, using private/business addresses, etc. By recording users' conduct, by coursework for new employees, and by tools such as URL filtering. control Applications.	1

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Human Resources and employees' awareness	19.7	Define rules and limitation on the use of social networks.	Define rules and limitation on the use of social networks: limitations on the publication of organizational information in the social media and public sites; representation of the organization in the social media; and access to social networks from the organization's systems.	User conduct in the social networks can define guidelines on the organization's representation in these networks, on divulging information and on precautions while accessing social networks from the organization's systems.	2
Human Resources and employees' awareness	19.8	Define and implement. sanctioning procedure following disobedience of data security rules.	The organization will define disciplinary procedures to deal with breaches of security by employees or contractors, will record disciplinary measures taken.	For example: an employee who breached clear instructions will be summoned, alongside his superior, to clarify matters with security elements. This may result in disciplinary measures up to termination of employment. Pay attention to cases requiring involvement of legal entities or authorities.	3
Human Resources and employees' awareness	19.9	Examine and update employee's authorizations when changing functions	Define procedures of labor mobilization, including authorization updates in line with new functions (removing unnecessary authorizations, defining new ones as required for the new function).	Authorization updates can be performed manually, by notifying the authorization elements in the organization, or automatically where authorization interfaces are integrated in the human resources systems (a computerized identification management system). In labor mobilization, it is preferable to delete all existing authorizations and define. new set.	1

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Human Resources and employees' awareness	19.10	Delete all authorizations and block user accounts at the termination of employment.	Define an updating process for the termination of employment, including removal of authorizations and user accounts.	Authorization updates can be performed manually, by notifying the authorization elements in the organization, or automatically where authorization interfaces are integrated in the human resources systems (a computerized identification management system). In employment termination, delete all existing authorizations, freeze, and later user accounts.	2
<p>20. Training and instructions: A Cyber-Defense policy is important to minimize cyber-attacks on the organization. Many current attacks are performed using social engineering, for example, penetration or Ransomware attacks, fishing via email, impersonation in order to perform authorized activities (money transfers), etc. the organization's employees are significant tools in an attacker's hands, therefore seminars and awareness raising activities are important organizational tools in coping with such risks. The organization is required to periodically instruct employees at all levels in Cyber-Defense. general seminars to raise awareness, as well as specific seminars to functionaries in sensitive positions. and to practice them regularly.</p>					
Training and instructions	20.1	Develop, record and implement. data security awareness policy	The organization will define data security awareness policy, including periodical refreshers, types of personnel to be instructed in various subjects, and follow up means.	Can be implemented by writing. seminars policy, including content, performance and follow up responsibilities. This policy will define various target audiences (new employees, key personnel, employees whose employment is terminated, suppliers, external elements, etc.), who is in charge of the seminars, control and supervision (signing, declaration, an examination, etc.), required achievement, frequency of instruction, and essential subjects.	2
Training and instructions	20.2	Conduct basic data security training to employees. 	The organization will conduct basic training, relating to proper use of information, data security rules, internal and external threats, including threatening signals.	Can be implemented by internal or external coursework, suited to the organization's policy and needs.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Training and instructions	20.3	Conduct specific data security training to functionaries accessing sensitive data.	The organization will conduct initial and periodical seminars, including (according to function): operating environmental security controls, operating physical security controls, practice in conduct during data and cyber security events, systems' suspicious behaviors, identifying malware.	Can be implemented by internal or external coursework, suited to job definitions, and the organization's policy and needs.	3
Training and instructions	20.4	The organization will raise employees' awareness of social engineering.	Verify that functionaries are aware of fooling and impersonation attempts of potential attackers.	Can be done in-house or by an external company. Such attempts can include "illegitimate" requests from support personnel, requesting information on behalf of somebody else, attempts to act without user verification, initiating requests in the social networks or via Emails, etc.	4
Detect					
<p>21. Recording and monitoring</p> <p>The Defense Methodology assumes that regardless of all defenses, some attackers will succeed in penetrating the organization. As part of coping with a cyber-event, the organization must be capable of identifying such events and treating them. The organization is required to record relevant activities in its systems, which may indicate cyber-events. In addition, the organization should monitor this documentation in a manner that will allow it to detect these events as soon as possible, for quick reactions and damage minimization. The controls are intended to define events, and create effective documentation and monitoring infrastructures.</p>					
Recording and Monitoring	21.1	Define, implement, and periodically review, recording and monitoring policy 		Recording and monitoring organizational policy, and supporting rules, such as data security monitoring center, event recording rules, etc.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Recording and Monitoring	21.2	Determine events to be recorded by the system (logged), and for which periods. These control records should form the basis for the debriefing of security events. Define which systems should be audited (servers, communication elements, applications, databases, etc.)	The organization will determine which events in its systems will be recorded within its data security systems, as well as monitoring rules, used in these events. It will determine minimum length of time of keeping these records, complying with state regulations.	Can be implemented by ex post factum characterization of common events.	2
Recording and Monitoring	21.3	Examine periodically the recorded event definitions and the effectiveness of the recording system	Examine periodically the working premises vis-a-vis changes in the organization's systems, to assure completeness of recording. In addition, examine periodically the recorded events normalcy, and their accord with the organization's definitions and needs.	A periodic examination of the recording mechanisms and their accord with the organization's systems. For central control system, it is possible to use automatic mechanisms to verify the activities and normalcy of the events recording system.	2
Recording and Monitoring	21.4	Employ mechanism producing event control records. At least record events from systems containing sensitive customer data, from systems critical to the organization's functioning, and from core systems (servers, communication elements, applications, databases, etc.)	The organization will ensure that infrastructure and applicative systems employ logs, and the records are stored for. spell defined by the organization. Control records will hold information such as event type, timing, source, user name. In any case, the organization will monitor sensitive systems, parts of its critical infrastructure, and those managing core processes.	Usually, infrastructure systems contain logging mechanisms. In cases of applications, verify the existence logging options. It is possible to operate central logging mechanisms, linked to the organization's systems, and logging events to. central database.	1

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Recording and Monitoring	21.5	The organization will define additional data required for logging its systems, including. unique identifier of each activity, command, and query.	A basic system log does not necessarily record all data required to investigate an event. Therefore, the organization should define events/ data required to be logged. Sensitive systems require. deep and detailed logging of activities, in order to create quality alerts.	Define fields to be monitored in various systems. Occasionally it is necessary to define monitoring at the development stages, or to expand monitoring databases in order to collect such detailed information.	3
Recording and Monitoring	21.6	The organization will implement. central monitoring and alert system.	Define and implement. central monitoring and alert system, to collect data from various systems and to centralize analysis, alert, and coping with suspicious events.	For example,. SIEM system, combining security information management (SIM) and security event management (SEM), and providing. real-time analysis of security alerts generated by network hardware and applications.	3
Recording and Monitoring	21.7	Logging mechanism will include, at least, data about the event, timestamp, source and target of the activity, user identifier, process identifier, success/ failure, file name.		For organization of value level. an up, verify that the activity log does record all required data. In most cases it is possible to use logging mechanisms already existing in infrastructure systems. In applicable systems, verify the existence of. functioning log.	1
Recording and Monitoring	21.8	Allocate enough logging storage space.	The organization will allocate enough storage space for its long term logging and monitoring needs.	Pre-plan data storage requirements. Perform periodical capacity planning.	2
Recording and Monitoring	21.9	Create an alert mechanism in cases of logging failures.		The organization will monitor its data security monitoring system, to be alerted when no events are recorded for. period of time from an information system that is normally monitored. Such cases can be defined as rules in most logging and monitoring systems (SIEM, Log Management).	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Recording and Monitoring	21.10	Define sensitive activities that the organization wishes to monitor.	This control is intended to ensure that the organization defined scenarios to be monitored, and is capable of obtaining such information.	Can be done by questioning the business elements about work processes and unauthorized activities. The following events and scenarios to be monitored can be gleaned from IT personnel: irregular activities in the network, such as access to sensitive files; multiple failed identification attempts; copying multiple files to local storage spaces, illegitimate behavior of supplier or outsourcing employee, etc. in order to monitor such events, use SIEM system as well as local reports, output from various systems, security cameras, questioning employees, etc.	2
Recording and Monitoring	21.11	Review and analyze periodically the control records. Report the findings to specific functionaries.	The organization will extract data security and trends reports, reporting to the management or to specific functionary.	It is possible to extract such reports from any data security monitoring system, such as SIEM	2
Recording and Monitoring	21.12	The organization will use automated mechanisms to identify suspected cyber-incidents out of monitoring records.	In order to detect suspicious events, it is necessary to generate alerts and indications from monitoring data collected from enterprise systems. Event that the organization has defined as suspects should be handled in accordance with the outline of the organizational threats.	Can be implemented using reports, queries and rules applicable to the monitoring database, or by dedicated monitoring system such as SIEM.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Recording and Monitoring	21.13	The monitoring system will collect control records from various data sources in order to get complete corporate picture.	The organization will implement 'Correlation Engine', aimed at integrating data from different information sources (different systems), enabling identification of lateral events and advanced attacks on the enterprise systems.	For example, combining data from the system and communication systems, from infrastructure and application systems, from various physical access control systems, surveying vulnerabilities and integrating inputs from cyber intelligence sources.	4
Recording and Monitoring	21.14	Protect control records from unauthorized access, change, or deletion.	The organization will secure the storing area, and toughen the monitoring array, to prevent the updating of log records.	Can be implemented by limiting access to the monitoring records storage, and servers.	2
Recording and Monitoring	21.15	Backup control records on periodical basis, store backup files away from the monitoring system.		The organization will define ongoing backup methods of the monitoring array definitions (backup monitoring rules and configurations), as well as of the collected logs.	3
Recording and Monitoring	21.16	Use cryptographic mechanisms to protect the integrity of records and control tools.	Log files will be stamped by digital stamping and hashing, to verify non-alteration.	Most SIEM systems support these functions. verify its proper functioning.	3
Recording and Monitoring	21.17	Make sure it is possible to retrieve and/or search records stored as far back as possible.	Periodically, the organization will ensure that old (as possible) control records may be retrieved.	For example, it is possible to extract report from the establishment of the system, to verify that such events exist in the monitoring system.	4
Recording and Monitoring	21.18	Implement user's session mechanism in the information systems.	Define the recording mechanism and employment rules of this mechanism, including cases when it is necessary to record, privacy rules and access authorization to the recording system.	Can be implemented by operating user's session system over workstation, installation on terminal or application servers.	4

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Recording and Monitoring	21.19	Implement mechanism identifying and alerting from attack attempts in real time.	These alert mechanisms will detect and alert on an attack attempt.	Can be implemented by defining SIEM rules, alerting from attack and data security events. And by establishing. security operations center (SOC)	4
Recording and Monitoring	21.20	Monitor incoming and outgoing communication to identify irregular or unauthorized activities.		Can be implemented by analyzing organizational firewall traffic and IPS, and correlate vis-à-vis external feeds to identify communication to suspicious servers.	3
Recording and Monitoring	21.21	Implement specific monitoring devices of user activities of high risk levels (as user with high security clearances).	The organization will characterize sensitive organizational functions, ensuring that these are covered by specific monitoring rules, in relation to sensitive activities.	It is possible to compare with. group of sensitive users within the Active Directory, or to load. list of such users to the SIEM array. It is possible to alert after defining any new ADMIN user within the DC.	3
<p>22. Security Controls Assessment: Security Controls Assessments are meant to assess the actual controls implementation, in line with this Defense Methodology. and to assess the defense effectiveness. It is desirable to perform the assessment by an independent organizational entity or an external one. The effectiveness can be assessed by penetration and vulnerability tests, Red Teams, etc. the controls are required to assess periodically that Cyber-Defense systems are properly defined and up to date with changes in the organization and possible cyber threats.</p>					
Security Control Assessment	22.1	Policy. write and implement. data security vulnerability management policy, review and update it periodically.	The organization will define. policy of vulnerability management, including: identifying and assessing vulnerabilities, correcting vulnerabilities, responsibilities, and ongoing follow-up.		2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Security Control Assessment	22.2	Procedure -Write. data security vulnerability management procedure, including assessing and correcting vulnerabilities.	The organization will prepare. procedures and plan portfolio, to implement and operate. data security vulnerability management array, emphasizing identification systems, tools and surveyors employment, sub-suppliers and employees' employment to deal with the findings. In addition the data security vulnerability management array will include one or more of the following tests: Security Control Assessment, malicious user test, internal threat assessment, and other tests defined by the organization.	The Security Control Assessment program will include various procedures and processes, intended to detect vulnerabilities,, follow up of correction processes and mechanisms, parallel process interfaces (data security update management, data security system configuration management, secured development, etc.). The organization will integrate in the data security vulnerability management program, penetration test simulating internal and external users, configuration assessment systems, etc.	2
Security Control Assessment	22.3	Assess system penetrability on. periodical basis	The organization will assess penetrability of infrastructures and applications (internal and external, if managed by the organization) on. periodical basis	Financial organizations, for example, conduct annual, even multi-annual, penetrability assessments of all their systems, thus being able to perform continuous follow-up.	3
Security Control Assessment	22.4	Appoint an independent company to assess penetrability.	The organization will employ external data security experts to conduct these assessments.	Occasionally one may conduct these assessments by an internal team, not subject to the IT but to. security not in charge of correcting the faults.	4
Security Control Assessment	22.5	The organization should employ an independent team to conduct penetration assessments, and Red Team exercises, to simulate attack attempts on its assets.	The organization will employ an external data security team, to simulate attack attempts, in order to test its controls and response capabilities.	This control can test the response capabilities of the monitoring teams, and the infrastructure and data security teams' capabilities to block such attempts in real time.	4

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Security Control Assessment	22.6	<p>Conduct continuous vulnerability assessments, according to the organizational vulnerability management process, by designated tool for all data systems (internal and external).</p> 		Can be implemented by installing security control assessment tool, and assessing every few weeks, months (it is possible to define specific timings to various environments).	2
Security Control Assessment	22.7	Verify that the security control assessment tool is always up to date, containing all vulnerabilities discovered and reported.	Verify that the assessment tool is updatable, licensed (thus regularly updated), and updated.	Can be assessed against update dates of the vulnerabilities list. Verify communication with the supplier's updating site, or the existence of mirror site within the organization.	2
Security Control Assessment	22.8	The organization should validate vulnerabilities detected by the automatic system, by an internal process, including an assessment of vulnerabilities identified in other systems.	The organization will define validation process, dealing, at least, with detected critical vulnerabilities, verifying, manually or automatically, the existence of these vulnerabilities in other systems.	For example, if critical vulnerability is discovered in Windows, or in the system's database, it is possible to assess non-updated servers, running the same version by tool.	4
Security Control Assessment	22.9	Conduct Credentialed Scans, with the vulnerability assessment tool	The organization will appoint Credentialed Scanner for the system being scanned, allowing thorough assessment of all processes and updates installed, as well as vulnerabilities in its toughening definitions.	Most security control assessment tools allow Credentialed Scan.	4

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Security Control Assessment	22.10	Verify the existence of an automatic tool comparing past and present vulnerability scans, to allow control and trend analysis.	The organization will conduct an automatic follow-up of detected vulnerabilities, in order to detect high risk systems, or systems with unsatisfactory controls implementation.	Can be implemented with the scanning tools or by an interface to third party systems (such as SIEM).	4
Security Control Assessment	22.11	Verify harmony of outputs of different security control assessment tools implemented in the organization, in order to obtain. full present situation of various vulnerabilities.	Verify that all vulnerabilities assessment and control tools are linked to. central system, in order to obtain. unified present situation of all vulnerabilities and controls.	Can be done by establishing an interface between vulnerability scanning and Patch Management tools to. central interface, such as SIEM, or. Data Analytics/ BI tools, in order to produce one encompassing vulnerability report.	4
Security Control Assessment	22.12	Integrate an automatic central fault correction mechanism	The organization will integrate. central system, to manage vulnerabilities and their correction.	Can be implemented by establishing interfaces between the vulnerabilities management array and the organizational reading system, or by using. designated system (GRC).	3
Security Control Assessment	22.13	Control the vulnerability correction process. Apply measurable objectives to correct vulnerabilities, according to their gravity.	The organization will define SLA objectives to deal with vulnerabilities, according to their gravity. In addition, define alerts in relation to deviation from time tables of vulnerabilities correction, vis-à-vis the measures and objectives defined (SLA)	For example, critical vulnerabilities will be corrected immediately, high vulnerabilities within. month, medium within three months, etc. In addition implement SLA alerts to calls opened in the vulnerability management array, and report about deviations from these objectives.	3

23. Proactive Cyber Defense:

Proactive cyber controls allow the organization flexibility in defending itself against varying attacks. The organization will collect updated data about cyber threats and coping measures, and information about its digital presence, translating the last into ad-hoc applicable controls. In addition, the organization will implement. deception array of potential attackers (honey traps and other luring and deception technologies) in order to confuse the attacker, reduce his motivation, trap him as soon as he penetrates the organization, etc. The organization will implement behavior patterns based analysis controls in sensitive environments.

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Proactive Cyber Defense	23.1	The organization will define and periodically update. proactive Cyber-Defense program.	A proactive Cyber-Defense program will detect new threats, adjust controls to detected threats, collect intelligence and other data, survey new controls.		3
Proactive Cyber Defense	23.2	The organization will collect up-to-date cyber threats and coping methods information.	The organization will learn from public information sources about new cyber threats, relevant to its business and technologies.	One can get access to information, free tools, tutorials and more at open sources such as Metasploit, security companies' sites, etc., and contact intelligence companies.	3
Proactive Cyber Defense	23.3	The organization will collect data about its digital presence (business activities, customers, internal users).	Such collection is intended to identify cases of sensitive data exposure on the Internet, including the "Dark Net."	Use the services of specialized companies.	3
Proactive Cyber Defense	23.4	The organization will use cyber threat information to devise and improve applicable controls.	The organization will map the changes necessary to its data security systems' definitions, as well as its infrastructure and application controls, to cope with new threats.	Changes may apply to networks, firewalls, applicative systems and interface definitions, etc. Update systems' rules following the updating of their definitions.	3
Proactive Cyber Defense	23.5	The organization will implement. luring and deception array of potential attackers.	The organization will integrate technologies to lure, deceive, and delay potential attackers, to improve its identification and coping capabilities.	Systems such as Honeypots, designated, monitored virtual servers, file stamping. Can be implemented in various ways, such as defining fictitious users, objects within the DC, intended to lure attackers, concealing files with "coveted" names, such as "Salaries," "Passwords," "Secret," etc.	3
Proactive Cyber Defense	23.6	The organization will integrate controls based on behavior pattern analysis (system and user) in sensitive environments.	The organization will integrate systems, identifying anomalies in the server and network levels of service and sensitive data environments.	Such systems can function at the server level (Advanced Threat Analytics) and network level (MacAfee, NTBA, STRM Sourcefire 3d, etc.)	3

Respond

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
<p>24. Events Management and Reporting</p> <p>The organization should be able to manage an ongoing cyber-event in a manner reducing damage, neutralizing the threat and returning to normal. This alongside debriefing the event, drawing lessons, and adjusting the defense array accordingly. Such controls are intended for this objective. In this framework, the organization will define coping measures in a cyber-event, reporting channels to employees about a suspected security event, the professional entity (within or without the organization) supplying professional knowledge, support and assistance in monitoring, identifying, investigating, and reacting to cyber-events. The organization will define reports to be produced in the occurrence of cyber-events and their endings (for example to the national CERT, and regulator), etc. Inspect response capabilities periodically, using tests defined by the organization.</p>					
Events Management and Reporting	24.1	Write and implement a reactive policy to events. Review and update the policy periodically.	The organization will write and implement a reactive policy to data security events, as part of its organizational data security policy, and will review and refresh that policy.	In writing events' treatment policy, define functionalities and response teams, gravity levels, and communication means with the authorities (the Police, ILITA, The Israel Law, Information and Technology Authority, The National Cyber Authority, the regulator, etc.). Define event managers (various functionalities may be in control during various events, such as ransomware attacks, threats to publish users' data, etc.). It is important to write this policy in cooperation with relevant third parties, such as regulators, suppliers, emphasizing cloud systems, outsourcing employees, etc. It is recommended to define situations during which a situation room should be opened, when and how to involve management, reporting frequency, appealing to the national CERT, Cyber-Defense Authority, recovery, etc.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Events Management and Reporting	24.2	Develop. cyber and data security event coping plan	The organization will develop. plan to identify, cope with and respond to cyber and data events, including: an outline of realizing response capabilities to security events;. description of capabilities to cope with events, response to the organization demands, considering its tasks and size, events requiring reporting; supplying measuring means of the organization's capabilities to cope with events; resources and management support required to maintain and improve response capabilities		2
Events Management and Reporting	24.3	Develop coping capabilities with cyber and data security events, including preparations, detection and analysis, interception and recovery.	These controls aims to assure that the organization maintains the knowledge and tools needed to debrief, contain, and manage an event effectively and to cope with its consequences.	Can be implemented by the security event coping plan, emphasizing the recruitment of professionals serving as. basis for detection and response to events, training the team to cope with various events (viruses spread, ransomware, coping with DDOS, leaked information, etc.). Can be implemented by debriefing tools or ERT's)	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Events Management and Reporting	24.4	Integrate automatic mechanisms to support coping with events.	Managing multiple events and alerts is complicated business. Therefore, it is required to automate as much as possible alert status follow-up, required activities, decisions, etc.	Can be implemented by linking command and control systems to events monitoring and detection systems. It is possible to define response procedures within command and control systems. Can be implemented by decision support systems, Work Flow management systems, or Ticketing systems. It is recommended that such tools will assist the organization in locating long time events, grave events not dealt with properly, and situation requiring immediate intervention	3
Events Management and Reporting	24.5	Record data security events and coping with, including data collection, activities and conclusions.	The organization will maintain centralized reporting mechanism, in order to have unified and full situation report of the event and risks evaluation.	Can be implemented centrally by SOC (Security Operations Center), collecting and recording data.	2
Events Management and Reporting	24.6	Define data security reporting channels for employees.	The organization will apply obligatory reporting procedures, formats, in cases of cyber-events	Can be implemented by instructing employees about data security events and their reporting procedures. It is recommended to approach the national CERT for assistance in response and recovery.	1
Events Management and Reporting	24.7	Define. functionary whose job is to supply professional knowledge, support, and escort in monitoring, detection, debriefing and responding to data security events.	The organization will appoint professional entity to serve as professional knowledge source, in the identification and debriefing of data security events.	It can be an internal or external entity, experienced in identifying, debriefing, and responding to events. It will guide the teams operating the events, sharing his experience in cyber-events.	3
Events Management and Reporting	24.8	Integrate mechanism providing accessibility to information about reactions to cyber and data security events.	The organization will provide access to file containing detection and response procedure in cyber and data security events.	Can be implemented by any data or documentation management system, or by printed copy.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Events Management and Reporting	24.9	Instruct relevant functionaries in reacting to security events.	The organization will train all entities involved in coping with data security events in identifying and responding to such events. These seminars will be refreshed periodically.	Such seminar portfolio should include response procedures, best practices and tools serving to make this information accessible during such events.	2
Events Management and Reporting	24.10	Integrate event simulations within training, to improve the teams' response effectiveness in crises.	The organization will simulate data security events scenarios, in order to test its readiness and prepare accordingly.	Some exercises will simulate guided events, and the teams' reactions will be measured by the exercise's controller. Other exercises will simulate events in production environments, with real means, such as phishing exercises.	3
Events Management and Reporting	24.11	Implement automatic mechanisms to provide realistic training environments.	The organization will simulate real data security events in environments simulating the organizational environment.	Cases can be simulated in testing environments or in designated external laboratories (a professional cyber laboratory).	4
Events Management and Reporting	24.12	In order to check effectiveness, Examine response capabilities periodically, using test defined by the organization, including simulation of real event. Record the outcomes of each periodical test. 	In order to test response capabilities to data security events, the organization will simulate real attacks, inter alia with automatic attack tools. The organization will record and derive lessons from these exercises, and produce debriefing report.	Can be measured by an event script, counting detected events, and response quality (minimizing damages, communication among entities, concentration, and operation, recovery). Events detection can be integrated with real penetration attempts carried out in the organization. Real attack tools will be used in the test.	3

Recovery

25. Business Continuity:

The organization's objective is to maintain business continuity and minimize damages from cyber-events. This is what business continuity controls are here for. The organization should verify fast recovery of its cyber infrastructures. Prepare alternative infrastructures (including availability and redundancy), periodically test and practice its business continuity plan. Effective, available, and reliable backups are critical to business continuity, and should be exercised regularly.

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Business continuity	25.1	Write, implement, review, and update. business continuity policy, regarding Cyber-Defense . 	The organization will prepare. business continuity plan, derived from its objectives and implementing controls and processes in order to achieve these objectives. The plan will take into consideration various disaster scenarios and critical processes. The organization will define those assets supporting critical business tasks and functions (physical and digital). The organization will define maximum spell of essential services closure before returning to normal (in emergencies). As part of the continuity plan the organization will define the time spell within which essential tasks will return to normal since the plan's operation.	The organization will write, implement, and periodically update. business continuity plan. This plan will define the organization's conduct in normal and emergency periods in order to ensure business continuity (including common indices, such as RTO) in cases of cyber-events. It is possible to use aids such as ISO 22301 standard.	2
Business continuity	25.2	Prepare required capacity planning for emergencies (computing, communication, support services).	The organization will ensure that systems and infrastructure intended for business continuity in emergencies, support the desired capacity for the required scopes and time spells.	Can be implemented following. mapping of critical services, defining recovery and survivability objectives of each service. Normally, the organization measures the required capacity in the alternative site, in terms of communication infrastructures, system infrastructures, applications, and licensing.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Business continuity	25.3	Instruct employees concerning business continuity.	The organization will instruct employees in business continuity procedures.	Refer to employees' functions in recovery, temporary gathering sites, logistics and operations, and recovery objectives of the team and organization levels.	2
Business continuity	25.4	Exercise the business continuity plan on a periodic basis.	The organization will prepare and conduct preparedness exercises, to test the effectiveness of the business continuity plan.	Can be implemented by exercising various scenarios. It is recommended that the exercising will include the IT aspects of the business continuity plan, such as telephone and computer communications, as well as complimentary aspects such as suppliers and (local and cloud) services, guided by the BCP plan. It is also important to raise emergency awareness, by considering the need and urgency of shifting new versions to the production environment, by being strict in escorting visitors, by trying to recover files, by exercising cyber-event management, decision making at the management level, debriefing and drawing lessons.	2
Business continuity	25.5	Exercise the business continuity plan by periodic simulations.	The organization will use simulations and involve employees expected to be involved in the recovery plan implementation.	In order to carry out simulations as close to reality, prepare disaster scenarios, operate the plan (in a reduced manner) in the DR environment, and test the validity of the plan	3
Business continuity	25.6	Test the continuity plan periodically and fill gaps discovered.	The organization will review and correct its business continuity plan periodically.	For example: testing program, performing partial shift to an emergency environment, or to various systems, in order to test the shifting processes.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Business continuity	25.7	Test the continuity plan in the alternative site, to familiarize the continuity team with the site and its resources, and to evaluate the site's capabilities to support activities requiring continuity.	The organization will prepare processes and procedures to familiarize and exercise the backup site, as part of exercising the business continuity.	Can be done by traveling to the backup site, becoming familiarized with the system stored there, and exercising the actual shift to the alternative site.	2
Business continuity	25.8	Use automatic tools to thoroughly test the continuity plan	The organization will use automatic tools allowing control and testing of the plan's effectiveness.	Such tools can be. control of the backup array, including failure alerts, control of High Availability, between the main and secondary sites, monitoring communications between sites, etc.	8
Business continuity	25.9	Perform. full system recovery as part of continuity plan testing.	The organization will perform periodically. full recovery from backup, of systems defined as parts of the Disaster Recovery plan.	For example:. full recovery into the backup environment. Following recovery, perform acceptance testing to verify full functionality. Including data comparisons, configuration testing, and working with the recovered systems.	3
Business continuity	25.10	Establish an alternative backup and computing site allowing. full recovery at the same security level as the main site.	The organization will establish and maintain. secondary site, containing systems' copies, as well as data and storing security systems, all supporting recovery and business continuity of critical processes.	Can be implemented by duplicating servers and survival environments in the alternative site. Virtualization technics etc.	2
Business continuity	25.11	In order to avoid both sites being attacked simultaneously, verify physical and logical separation.		The organization will verify. proper geographical distance between both sites, as well as among computer networks and support infrastructure.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Business continuity	25.12	Define the backup site in. manner supporting the recovery plan	The organization will define systems and communication lines in. manner allowing. fast and effective recovery.	This can be implemented by High Availability systems in various configurations, allowing fast data duplication and availability post recovery in the alternative site.	2
Business continuity	25.13	Identify potential accessibility problems to the alternative site in cases of regional disasters, and take proper preventive steps.	The organization will verify site accessibility in cases of disaster.	For example verify the existence of several approaches, survivability to earthquakes, and remote accessibility.	2
Business continuity	21.14	Prepare backup site infrastructure agreements, containing priority of service clauses, according to the organization's recovery objectives.	The organization will verify that its service agreements contain clauses committing the supplier to service and response times compatible with its objectives.	It is possible to verify that the SLA agreements with the backup site supplier system programmers' response and recovery times are compatible with the organization's service RTO. It is possible to dictate first priority in critical services' recovery.	2
Business continuity	21.15	Verify the alternative site's preparedness to function as. main site, and support essential tasks and business functions.	The organization will verify that all services (including support and infrastructure) in the backup site are available and functional at any given time.	Can be verified by preparing detailed tagging lists for support and infrastructure systems, and by periodical normalcy tests (as well as during exercising).	2
Business continuity	25.16	Prepare backups to communication networks, and verify the existence alternative communication services, in order to reduce dependence on. single point of failure.	The organization will verify the existence of an alternative communication network between its main and backup sites, as well. dual communication link to the main site.	Can be verified by purchasing and operating backup communication lines, thus minimizing dependence on. single point of failure.	2
Business continuity	25.17	Require alternative, emergency service suppliers to prepare and periodically test. business continuity plan.	The organization will verify that suppliers' recovery objectives are compatible with its own.	Suppliers can provide their own emergency plans, including recovery objectives of services supplied to the organization.	2

Family	ID	Monitoring	Complementary Explanation	Monitoring application example	Control level
Business continuity	25.18	Prepare and protect backups of the user, system, and documentation levels.	The organization will back up all critical business data, and ensure their availability, integrity, and confidentiality.	Backup disks, tapes, and cloud.	1
Business continuity	25.19 	Verify backup reliability and availability.	The organization will ensure reliable and available backups.	Can be done with periodical recovery tests.	2
Business continuity	25.20	Retain. backup copy of critical data away from the main site.	The organization will ensure that backup copies are retained in. remote site, protected from environmental disasters (fires, etc.).	Can be done by directly backing up to. remote site, or by regular delivery of the backup media to that site.	2
Business continuity	25.21	Implement. transaction recovery mechanism for transaction based systems.	The organization will install. mechanism to recover failed transactions due to system failure or. shift to. backup system.	Can be implemented in. variety of configurations: double writing configuration (two parallel transactions in both main and backup systems), verifying. transaction post-sending, retaining, and tagging failed transactions. In Queue Management Systems, the queue can be backed up.	2
Business continuity	25.22	Verify. recovery capability to. known operational status.	Verify the existence of mechanisms enabling recovery of data or configuration to. known status.	Can be performed by. configuration back up at. point of time (before implementing changes), and by determining data recovery points, and rollback mechanisms.	3
Business continuity	25.23	Verify service and critical infrastructure redundancy.	The organization will verify redundancy of critical services and infrastructures, in order to minimize dependence of. single point of failure.	Can be implemented by redundancy of critical infrastructures, such as communication equipment, main network services, security and storage systems, etc.	3





APPENDIX A \\

EXAMPLE OF RISK ASSESSMENT EXECUTION FOR AN INFORMATION ASSET

In the example below the calculation is: Risk = 3i + P = 3X3 + 2

	Question	Sample Answer	Weighted Score
Impact Level Questionnaire (intensity). This questionnaire appears on page 26 in the document.	What is the level of damage caused to the organization following disclosure of information from the system? C	2	
	What is the level of damage caused to the organization following the disruption of information existing in the system? I	1	Maximum value 3
	What is the level of damage caused to the organization following a long-term system shutdown ? A	3	
Exposure Level Questionnaire (Probability). This questionnaire appears on page 28 in the document.	How many users are in the system?	2	The average value 2
	Who are the system users?	4	
	How many interfaces does the system have?	1	
	What is the nature of the system interfaces?	1	
	The type of information existing in the system	3	
	Remote access to the system.	1	
	System user permissions compartmentalization level.	2	
	Current infrastructure	3	
	Updates and security patches	4	
	Physical Security	2	
	Weighted System Risk Score		3*3+2=11

After answering the above questionnaire for all the assets of the organization, the following list is obtained:

Probability (P) / intensity (I)	4	3	2	1
4	16 System A	13	10 System C	7
3	15	12	9	6
2	14	11 System B System D	8	5 System E
1	13	10	7	4

APPENDIX B \\

TOOLKIT FOR THE IMPLEMENTATION OF THE DEFENSE METHODOLOGY

In order to assist with the implementation of the Defense Methodology and make it accessible to various target audiences, a toolkit will be developed under the National Cyber Security Authority (NCSA). In addition, various economic entities may develop toolkits, as is customary in similar cases around the world.

The toolkit that the NCSA plans to develop consists of:

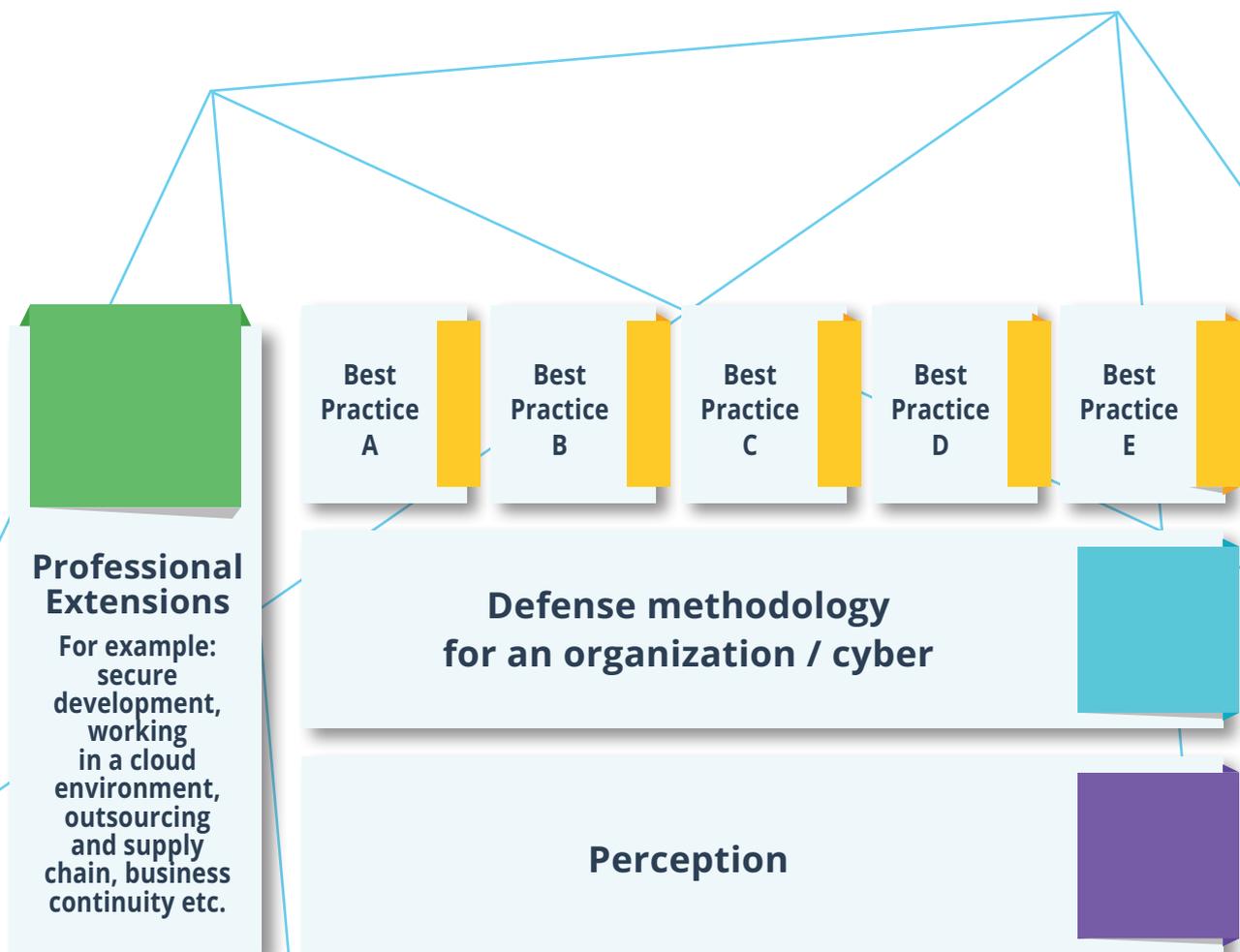
1. An automation process of the Defense Methodology through a convenient and efficient technological platform.
2. Generic forms and procedures ready for use by the organization, as for example a corporate policy document referring to Cyber-Defense aspects, Defense Methodology controls procedure, form templates, and more. The organization must **adapt** these examples and templates to its needs.
3. A risk assessment calculator, for the automation of some simple formulas of the Defense Methodology.
4. Examples of cyber assets mapping.
5. Enrichment information for controls.
6. Best Practices for selected controls.
7. Training kits for various target populations.

It is possible to view a toolkit that supports the Defense Methodology according to the following hierarchy:

- **A National Perception** - on the basis of which we write the Defense Methodology for the organization.
- **A Defense Methodology** - presents the various protection issues at the basic level (e.g. monitoring, awareness, networks separation, supply chain management, etc.)
- **Best Practices** - on the basis of this Methodology , we will write together with you specific guidelines for technology / service etc. such as Best Practice for hardening DB servers of a particular type or for working correctly with WIN 10 operating system, etc.

- **Professional Extensions** - alongside the Defense Methodology there will be extension documents that provide additional information which is not dependent on a specific technology (Best Practice), but, on the other hand, is more comprehensive and detailed than the basic requirements of the Defense Methodology ('professional extension').

The above information will be made accessible to the field in various forms (guides, online courseware, One pager for small businesses, training courses, etc.)



APPENDIX C \\

CONTROLS FOR THE DEFENSE OF A CATEGORY A ORGANIZATION - HIGHLIGHTS FOR IT SERVICE PROVIDERS

Family	Header	Monitoring	Complementary Explanation
Management Responsibility	Corporate governance:	Examine periodically the organization's approach to information security and Cyber-Defense management and its implementation.	In the framework of this monitoring, examine the security controls implemented in the organization as well as the information security and protection policy of critical business processes of the organization.
Preventing Malicious Code:	Detecting and preventing malicious code on endpoints and servers in the organization.	Implement tools to detect and prevent malicious code on endpoints and servers in the organization. These tools will be run in active protection mode and periodic scans will be performed as well.	Since some artifacts may penetrate the security mechanisms, ensure that controls for handling malicious code will also be applied at the workstations level.
Preventing Malicious Code:	Automatic updates	Run automatic updating of all systems for identifying and preventing malicious code within the organization.	The organization will activate automatic updates from a central server, managed by the organization or by a recognized service provider. These updates will keep the protection tools constantly updated.
Encryption:	Encryption Criteria	Define uses that require encryption and the necessary encryption type, in accordance with laws, guidelines, procedures, regulations and business commitments.	The organization will define what information and systems should be encrypted and record the configuration of the information encryption. The requirements will be derived from the requirements applicable to the organization or from information retention requirements.
Protection of workstations and servers:	Hardening Policy	Define, document and implement a hardening policy for workstations and servers, which meets the requirements of the organization's information security.	The organization will define hardening requirements for systems within the organization with an emphasis on the basic requirements, the frequency of updates and the level of classification and then document the requirements in an overall framework which will serve as a basis for writing the hardening procedures.

Family	Header	Monitoring	Complementary Explanation
Protection of workstations and servers:	Hardening Implementation	It is necessary to define the system configuration to provide the minimum functionality required (while blocking unneeded functions, ports and protocols).	The organization will define hardening procedures for each system and server type, based on acceptable practices to include, at a minimum: <ol style="list-style-type: none"> 1. Reduction of the system's attack surface by blocking unnecessary ports; 2. Turning off unnecessary services; 3. Removing guest user accounts; 4. Preference to using secure communication protocol between servers; 5. Getting email updates in an orderly manner; 6. Blocking sensitive functions of the system; 7. Sending system events logs to a monitoring server ; 8. Blocking software installation by unauthorized users.
Public cloud computing:	Shared Responsibility	It is necessary to understand the division of responsibilities between the service provider and the organization, and implement protection monitoring accordingly.	When using public cloud services there is a division of responsibility for cyber protection between issues under the responsibility of the supplier and issues remaining under the responsibility of the customer. This division of responsibility depends on the nature of the service and the implementation model. The organization has to understand what are the issues that are within its responsibility and implement the consequences of this responsibility.
Public cloud computing:	Sharing sensitive information	Make sure that no data, which under the regulation and responsibilities of the organization must not be transferred, is transferred to the cloud services.	There is data that the organization is prevented from transferring for storage or processing in public cloud services due to regulatory considerations or Commitment to third parties. Prior to transferring data to the cloud make sure that such data are not kept or transferred to the cloud services.
Protecting the information:	Protection of information stored on shared resources	Prevent unauthorized or unintentional data transfer via shared system resources.	The organization must prevent the transfer of information in an unauthorized manner, e.g. by using shared folders, e-mail, removable media etc.
Network security:	Managing connections (Sessions) - at network level	The organization will operate technological devices in order to protect services against Denial of Service attacks.	Defend against Denial of Service attacks (DOS) of various types, such as loading the computing resources to collapse, loading the communication bandwidth, loading the website to crash and more.

Family	Header	Monitoring	Complementary Explanation
Network security:	Sessions Reliability	Make sure that the Address Translation Service (DNS) is provided by a trusted server (intra-enterprise and extra-enterprise.)	The organization will allow obtaining Address Translation Service (DNS) only from a secure internal server. In order to prevent erroneous communication routing (intentionally or unintentionally) to hostile targets.
Network security:	Network Limits	It is necessary to limit the number of communication channels outside the system.	The organization will reduce and unite communication channels to ensure better control over the connections to the system.
Network security:	Network Limits	Block by default all network traffic and allow manually any desirable traffic by means of exception rules.	The organization will define the filtering rules of network traffic so as to block by default all traffic not explicitly defined as allowed.
Network security:	Network Limits	Use separate network addresses (different sub-network) to connect to different security zones.	The organization will determine that each sub-network will have a separate address range, which will be published to the firewall and routers.
Access Control:	Users Management	Set up user accounts that support the business functions of the organization.	At the very least, separate the 'Administrator' account from a 'user' account. It is also necessary to set up users who manage the system security functions (such as creating users, managing access and system privileges, managing the information security systems, etc.).
Access Control:	Permissions Management	Define and enforce logical access privileges to the system and the information in accordance with the access control policy.	The access control can be done on a personal level (identity-based), or the role level (role-based), and aims to control the access of entities (users or computer processes) to objects (files, records, devices etc.).
Human resources and employee awareness	Employees Etiquette	It is necessary to set rules of conduct in work with the enterprise information systems. These rules define the responsibilities and the rules of proper use of the enterprise information systems, with an emphasis on sensitive systems.	The organization will define behavior practices with respect to information systems and will distribute them to all the employees.
Human resources and employee awareness	Managing permissions during recruitment / mobility / departure.	Review and update the access rights of an employee while moving from job to job .	Define updating processes of employee mobility and updating permissions in accordance with the new role (removing unnecessary permissions and establishing the required permissions for the new job).
Security in procurement and development	Security requirements in procurement and in systems development	Supply chain security - require service providers to comply with corporate security requirements, regulations, standards and guidelines.	The organization will ensure that service providers comply with the organization's compliance requirements as well as with regulatory requirements applicable in the countries where the organization operates.

Family	Header	Monitoring	Complementary Explanation
Physical and environmental protection	Emergency Lighting	implement and maintain automatic emergency lighting, which will be activated in the event of a break or disruption in the power supply and will include emergency exits and evacuation routes in the facility.	
Physical and environmental protection	Fire Protection	Implement and maintain resources / systems for fire detection and suppression for the information systems which have an independent energy source.	
Documentation and Monitoring	Monitoring mechanism.	Activate a documentation mechanism that produces control records on incidents in the organization. It is necessary to record, at least, events from systems containing sensitive customer information, performance-critical enterprise systems and core systems (servers, communications components, applications, databases, etc.).	The organization will ensure that infrastructure systems and applicative systems activate an events listing mechanism, and that records are kept for a period set by the organization. The control records will contain information such as the type of event, when it occurred, the event source, the user name. In any case, monitor the sensitive information processing systems, which are part of the organization's critical infrastructure, or that manage the organization's core processes.
Documentation and Monitoring	Monitoring mechanism.	The documentation and monitoring mechanisms will include, at a minimum, information on the nature of the act committed, timestamp, source and target of the operation, a user ID, process ID, failure / success, mixed file name.	
Event Management and Reporting	Handling cyber-incidents and information security	Define reporting channels of employees to the bodies in charge in order to report suspected security incidents.	The organization will apply procedures on events that require reporting as well as the manner of reporting about an event defined as a cyber-incident.
Business Continuity	Resources availability	perform backups at user and system level and a system and documentation and ensure the protection of the backups.	The organization will perform a backup of all critical information in the information systems which support the business processes and will guarantee the availability, integrity and confidentiality of the backups.

APPENDIX D \\ STANDARDS COMPLIANCE

The Defense Methodology draws its knowledge base from accepted international standards, such as NIST 800-53 and ISO 27001. In order to make it easy for organizations to adopt the controls that appear in this document, the National Cyber Security Authority (NCSA) has mapped the existing controls to equivalent controls in the aforementioned standards. In particular, an organization that complies with the Defense Methodology and requires ISO 27001 accreditation standard can use the standard compliance appendix.

Later on, in parallel with the development of the corporate Defense Methodology, the National Cyber Security Authority (NCSA) will map the controls opposite leading domestic and international standards. Among the most important standards to be mapped soon are the following:

- Proper Banking Conduct Circular 357 + 361
- Cyber Risk Management Circular of the Capital Market Department
- Guidelines of the Israel Law, Information and Technology Authority (ILITA)
- ISO 27032

COMPLIANCE WITH ISO 27001

In view of the fact that this standard was constructed through relying much on international standards and in particular on the ISO 27001 standard, the completion which is required from an organization that implements this Defense Methodology in favor of full compliance with the requirements towards a certification Review is not large.

In order to facilitate for organizations that are certified or are considering to begin an ISO 27001 certification process, attached hereby is a conversion table, which reflects the Defense Methodology controls against the Statement of Applicability of the Standard. This table is on the National Cyber Security Authority (NCSA) website.

APPENDIX E \

CRITICAL PROTECTION CONTROLS FOR ACHIEVING A HIGH SCORE IN A SHORT TIME

The Defense Methodology defines a risk management process, and subsequently a requirement for exercising controls in the framework of a work plan. On the other hand, in some organizations there is a need to focus the first activities on performance. These activities include, in fact, the controls with the highest 'cost-benefit'.

The SANS Institute is considered one of the world's leaders in critical protection controls definitions, which are the most effective controls (CSC - Critical Security Controls). The implementation of controls, which cover 20 subjects, provides the organization with an 88% response from known assaults.¹

An organization that wants to get a quick snapshot of its defense preparedness can go over the critical protection controls, which are marked with a key symbol in Chapter 6 as part of the various control families.



The controls in this document were based on the same logic, but they do not necessarily represent the key controls of the SANS Institute.

Family	Detection
Risk Management and Risk Assessment	2.1.
Access Control:	4.2, 4.4, 4.17
Protecting the information:	5.1.
Protection of workstations and servers:	6.5.
Preventing Malicious Code:	7.1 ,7.2 ,7.3 ,7.9
Encryption:	8.6
Network security:	9.1 , 9.9, 9.12, 9.24, 9.25
Separation of Environments:	10.2, 10.4
Public cloud computing:	11.4, 11.6
Media Security	15.7.
Supply chain and outsourcing	16.2.
Security in procurement and development	17.14
Physical and environmental protection	18.6.
Training	20.2.
Documentation and Monitoring	21.1.
Security controls assessment surveys	22.6.
Event Management and Reporting	24.12
Business Continuity	25.1, 25.19

¹ <https://www.sans.org/critical-security-controls/history>

APPENDIX F \\

THE CONTROLS BANK

The controls bank is a significant element of the Defense Methodology . The bank, established on the basis of global common standards, contains many elements intended to enhance the understanding of the organization in implementing the controls.

For reasons of convenience and efficiency, necessary layers of information were inserted in the body of this document in order to implement the Defense Methodology. At the same time enriching layers of additional information have been set and written about every control. These layers currently are:

1. **CIA** - information security aspects which are protected by the control - availability, integrity or confidentiality.
2. **Cyber Kill Chain** - the stage in the attack chain where the control plays a role.
3. **Assets Categories** for which the control is relevant - IT, OT, services or databases.
4. **The risk levels** at which implementation is required - as the level of risk of an asset is higher, so controls providing a higher level of protection will be required, adapted to the relevant risk to the asset (levels 1-4 derived from the third stage of the risk management process described in this document).
5. **Control Type** - A control can be a guiding control (such as a procedure), preventive control (such as malware filtering systems), or detecting (such as monitoring and alarm systems).
6. **Control compliance with common standards** (in the first stage of the Defense Methodology publication the controls are mapped to standards ISO 27001 and NIST 800-53).

Extended and supplemental information on controls chapters can be found on the National Cyber Security Authority (NCSA) website.

APPENDIX G \

COPING WITH A SIGNIFICANT CYBER-INCIDENT

The Defense Methodology assumes that it is impossible **to guarantee complete protection** from cyber-attacks. Therefore, the controls chapters are designed to prepare the organization to cope with and recover from cyber-incidents with minor damage. On the other hand, in light of past experience we know that management of significant cyber-events is a professional field that requires specialized knowledge, tools, infrastructure and specialized professional training, which do not exist in every organization. The National CERT was established under the NCSA in order to assist organizations in dealing with such events. The CERT's mission is to enhance the cyber resilience of the Israeli economy by providing initial assistance and treatment for cyber threats as well as to coordinate and obtain relevant information from the various bodies in Israel and abroad.

CERT roles and activities:

- Incident Handling – starting with reporting, assisting and coordinating cyber-incident handling, up to assistance with recovery and investigation.
- Vulnerability and Artifact Handling - receiving artifacts, carrying out research to understand them and dissemination of methods and ways to handle them.
- Coping with and prevention of cyber threats - through proactive activities to detect, identify, and investigate them.
- Developing and disseminating knowledge for protection to target audiences - including tools and technologies for information sharing.
- Information and awareness raising - the general public, specialized audiences and the professionals engaged in cyber security.
- Developing and nurturing relationships with equivalent bodies in the world - exchange of information, Defense Methodologies etc..

Application for assistance to recover is possible, inter alia, through the following means:

A) By email: team@cert.gov.il.

B) By phone: 0723990800

C) By filling the form available on the CERT website at:
<https://cert.gov.il/ContactUs/Pages/ContactUs.aspx>



PRIME MINISTER'S OFFICE
NATIONAL CYBER DIRECTORATE
NATIONAL CYBER SECURITY AUTHORITY



מפל