



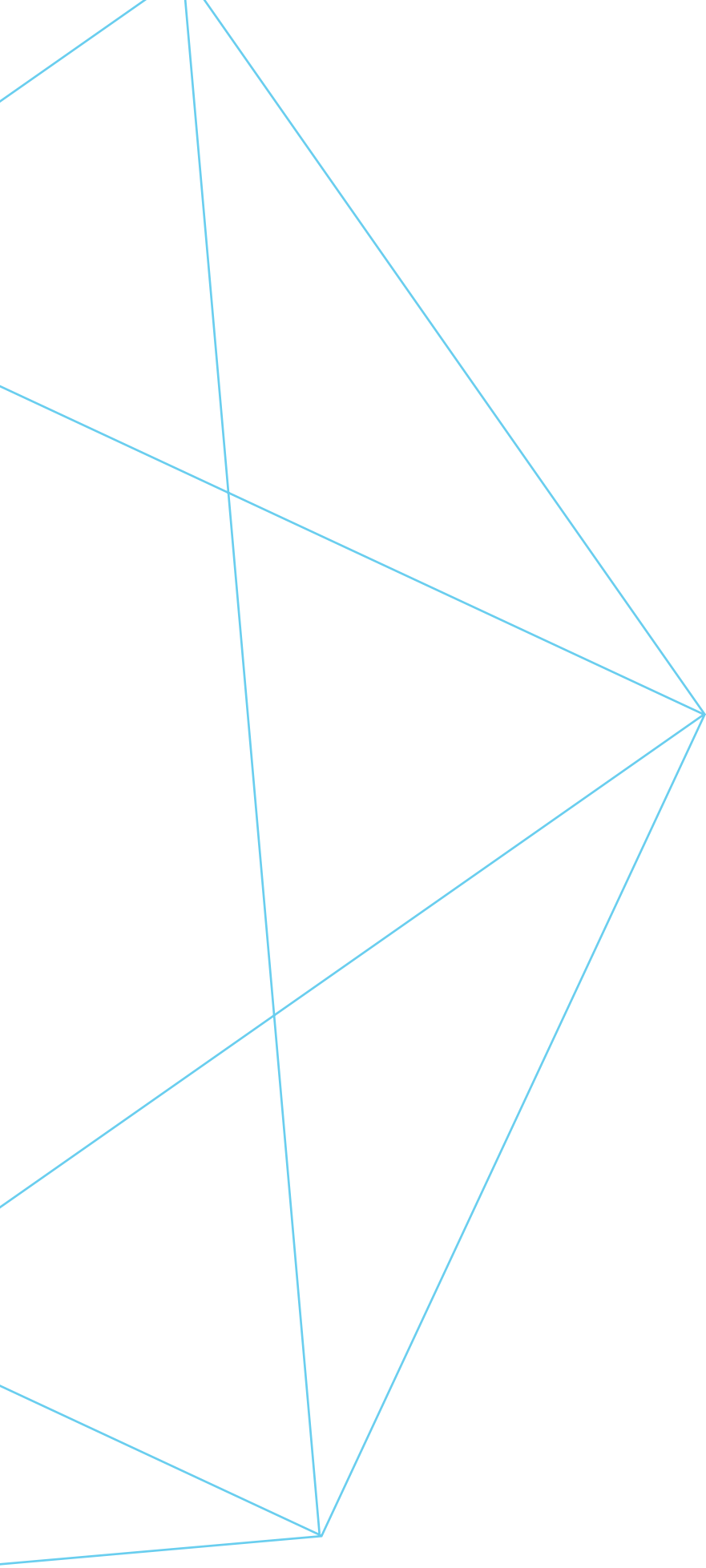
The Prime Minister's Office
National Cyber Directorate
National Cyber Security Authority

Addendum to the Organizational
Cyber Security Methodology

Use of Cloud Services

Version 1.0





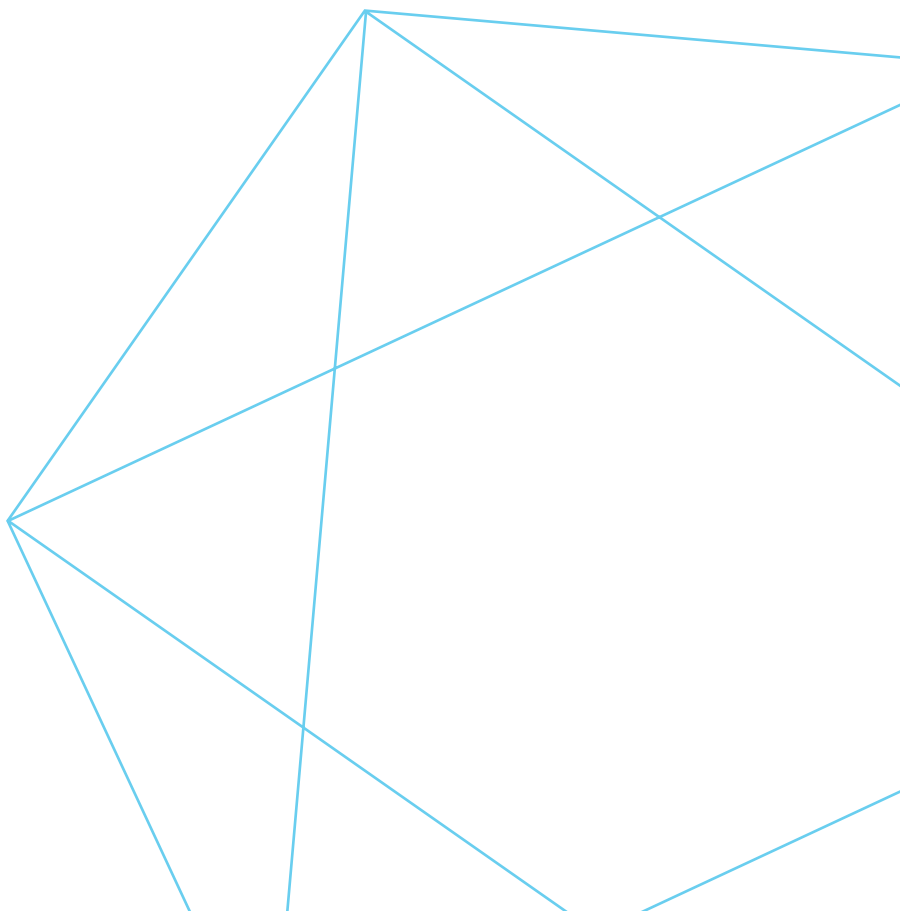


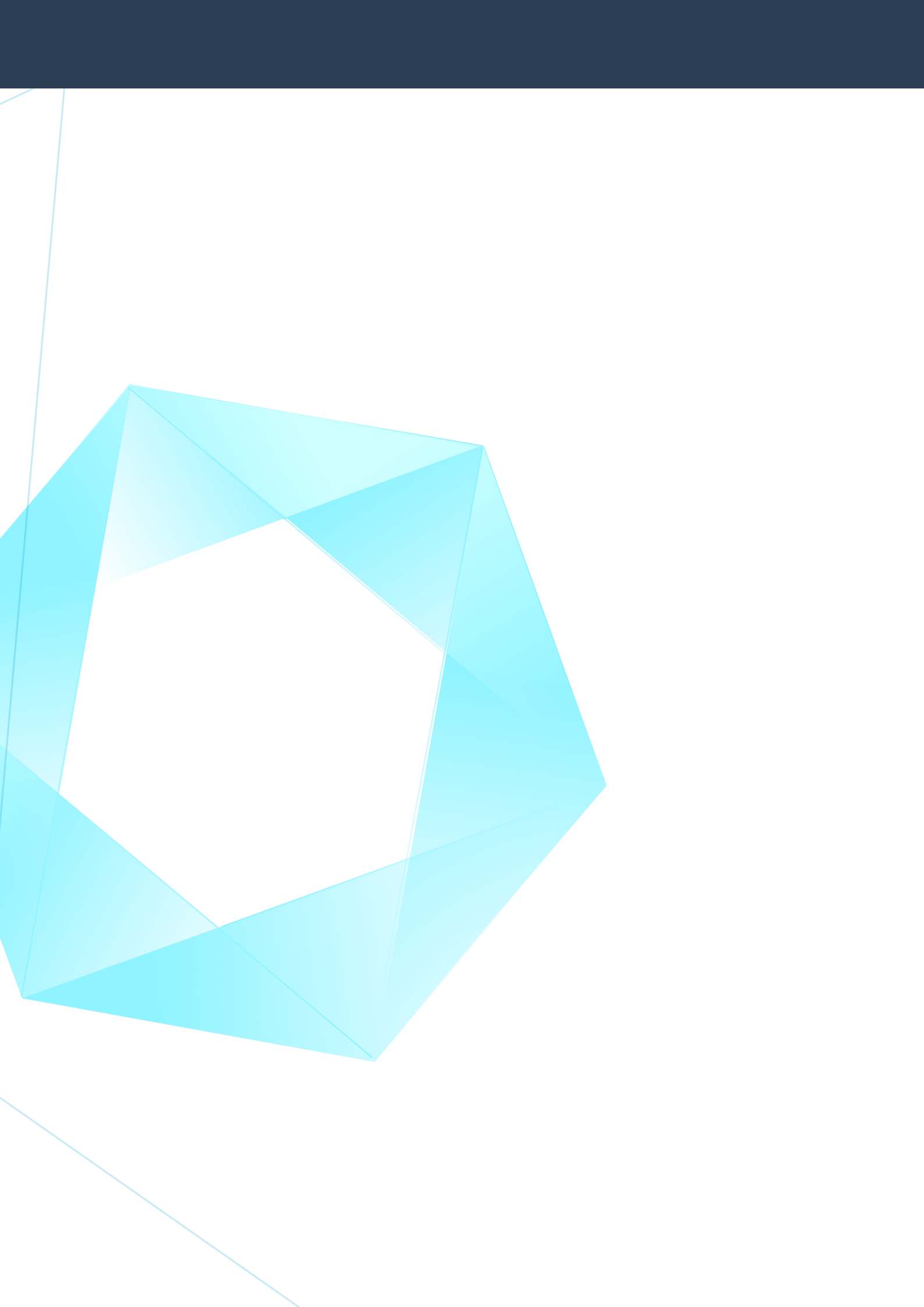
The Prime Minister's Office
National Cyber Directorate
National Cyber Security Authority

Addendum to the
Cyber Defense Methodology for an Organization

Use of Cloud Services

Version 1.0





Contents

Introduction	7
Background	8
Cloud Service Terminology	9
Chapter 1: Designing a Security Plan for Cloud Services	13
Stage 1.1: Mapping Assets and Information Gathering	13
Stage 1.2: Risk Assessment	17
Chapter 2: Security Controls for Cloud Services	20
2.1 Cloud Access Security Brokers (CASBs)	20
2.2 Receiving Cloud Services from Several	
Providers Concurrently	20
2.3 Security Controls for Organizations Using	
Cloud Services	21



Introduction

This document is an **expansion** of the **Cyber Defense Methodology for an Organization** disseminated by the National Cyber Security Authority. It provides detailed and complementary professional content on the particular topic of cyber security.

This document provides some background to the topic and its context relative to aspects of cyber security. The document also provides appropriate working methods for use and the relevance to the topic discussed for the purpose of strengthening and augmenting cyber security.

The document is intended for Chief Information Security Officers (CISOs) and should be viewed as an auxiliary organizing tool and guideline when a CISO constructs an organizational security plan.

In general, this document does not refer to security product manufacturers or detailed Best Practices (BP) to strengthen security by means of technical definitions. To this end, we recommend using the manufacturers' documents or the relevant BP document, if published separately by the National Cyber Security Authority.

Background

In the realm of information technology, the growing trend for organizations and end users is to avail themselves of cloud services. This is seen in the use of technologies applied as cloud services both through new applications provided by the cloud manufacturers and through the adoption of business strategies which convert or shift existing computing activity to operating out of cloud-based applications or infrastructures.

According to a survey published in February 2017 by Gartner, a globally leading firm in market surveys in the ICT world, we can expect an 18 percent increase in the use of cloud services in 2017 (with global expenditures likely to reach about \$246.8 billion). Gartner further anticipates that by 2020 half of all outsourced transactions of IT services will be cloud service related.

Many organizations are undergoing a fundamental change in their use of IT services. To date, most applications have been maintained, assimilated, and sometimes developed by the organization's own IT department. Now, however, it is evident that business units in organizations are promoting separate channels to build or consume IT services for supporting business activity using the cloud model.

The cloud services currently provided are many and varied and change at dizzying speeds. The implications and emphases that CISOs must consider when determining and applying appropriate security measures are likewise many and varied.

This document is intended for CISOs and is an addendum to the Cyber Defense Methodology for an Organization disseminated by the National Cyber Security Authority in 2017. The goal of the document is to present recommended working methods for CISOs who are charged with constructing a security plan while referring specifically to the cloud services that organizations receive and use.

Cloud Service Terminology

1. Cloud computing refers to a situation in which remote hardware / software resources are used via a public or private network.

Term	Explanation
CSP	Cloud service provider
CSC	Cloud service customer
CSN	Cloud service partner
Cloud portability	The possibility of moving an information application from one cloud service provider to another
Elastic computing	The use of resources and the possibility of expanding and reducing as needed
Cloud middleware	Software that mediates between various cloud service providers
Openstack	Open code software allowing automation in creating a cloud environment, including a storage facility, a communications facility, and management programs
PPU	Pay per use
RTO	Recovery time objective, relating to the availability to which the cloud service provider is committed
SLA	Service level agreement: the service agreement relating to the service level to which the service provider is committed
Vendor lock-in	Type of contract with cloud provider and the possibility of ending the contract

2. There are several **cloud service** models, the most prominent being:

2.1 Colocation: If a company prefers to save on building its own server room that meets the most stringent of standards, such as a reinforced underground structure, which requires a great deal of investment in electrical, cooling, and firefighting infrastructures and other elements, may prefer to store its computing equipment in an appropriate facility of a well-known provider based on a model called colocation. Clients are provided the area where their computing equipment will be stored, electricity and air conditioning, as well as fire protection and 24/7 physical security, but must acquire, install, and maintain their hardware on their own.

- 2.2 **IaaS** (Infrastructure as a Service): This is the basic and most common service model for companies and organizations. The main objective is to avoid having to build computer rooms or buy and maintain hardware equipment, including storage facilities, servers, communications components and information security components, and instead to receive services for payment according to usage, based on a model of virtual objects that can be controlled using a service interface.
- 2.3 **PaaS** (Platform as a Service): In this model, in addition to hardware and infrastructure, the cloud provider also gives the client a platform of basic software packages to allow an app development environment, test the client's products, and enable computing services from the platform.
- 2.4 **SaaS** (Software as a Service): In this model, the cloud provider supplies software and infrastructure, as well as the client's end applications. The app is bought from a company specializing in a particular applications field.
- 2.5 **DaaS** (Data as a Service): In this model, the organization consumes information from a database in the cloud and integrates it into its own information system. For example, an electric company planning its future production outputs may integrate information about the weather forecast for the next few days. The company can connect to the database, which may be stored in the cloud, and retrieve the relevant information as a service from an entity selling it. In this case, the organization must verify the information to ensure its reliability.
- 3. **SECaaS** (Security as a Service): This is a business model for consuming security services through the cloud to save on the costs of HR, hardware, software, and licenses. The services provided usually include identification, malware blocking, preventing network breaches, monitoring, and incident responses.
- 4. It is common to refer to four cloud-type **deployments**:
 - 4.1 **Public cloud**: Context in which cloud services are provided by means of an infrastructure (hardware, software, and applications) that is shared and open to all, sometimes even for free. While there is logical and sometimes physical separation and differentiation among clients and accounts, this is a pooling of resources.
 - 4.2 **Private cloud**: Context in which cloud services are provided by means of an infrastructure (hardware, software, and applications) accessible only to certain customers. Sometimes the infrastructure is located on the client's own premises and sometimes on the premises of the cloud provider. Communication and access to the infrastructure are provided exclusively to a single client whose involvement in its management is likely to be high.
 - 4.3 **Community cloud**: Context in which a certain sector or several organizations with a shared interest come together to receive cloud services specific to them.
 - 4.4 **Hybrid cloud**: The situation in which a client uses a private cloud for certain applications and does the same with a public cloud to connect the information or applications with other applications or information.

5. In cloud computing, there are two architectures for realizing the cloud:

5.1 **Single-tenant:** Depending on the type of cloud service and deployment, the client's use is exclusive, without splitting or sharing it with other users within or outside the organization. This may be manifested from the use of hardware to the use of an application developed exclusively for the client (generally in the deployment of a private cloud).

5.2 **Multi-tenant:** In this case and based on the type of cloud service and deployment, the client shares resources with other users, sometimes within and even outside of the organization.

6. To optimally carry out an organization's activity with a cloud provider, it is necessary for the organization to allocate professional personnel. Below are some job titles and their descriptions. Their implementation will be determined in every organization according to its resources and its volume of activities as a consumer of cloud services.

Job title	Description
CCO Chief Cloud Officer	Manages organizational cloud activity; is in charge of the information map and the cloud services and locations; contracts with cloud providers (together with the organization's acquisitions manager), and characterizes the needs for the cloud providers with regard to the following dimensions: • Information: storage method. • Service and required availability, as defined by the business factor. • Characterization of information traffic to and from the cloud.
Cloud Applications Manager	In charge of collecting the organizational requirements of the business units for cloud applications and passing those to the CCO and to the CISO.
Cloud Providers' Integration Specialist	In charge of information security with regard to the information transmission channels, encryption of information, and planning the security of the transfer of information as a whole between the cloud and the organization or between one cloud and another.

Job title	Description
Cloud Information Security Specialist	In charge of infrastructure security in the IaaS model and of assimilating information security components: • Security of stored information: in charge of data encryption of de-identification. • In charge of security in relation to information access, operating systems, and databases. • In charge of providing permissions based on the need to access information and perform actions on the information in the cloud. Securing the coding in SaaS/ PaaS.
Cloud Information Control Specialist	IaaS: control of network topology and definition of means of information security. PaaS: control of the development of secure code/application.
BCP specialist	Writing business continuity procedures for applications and information stored in the cloud.

Chapter 1: Designing a Security Plan for Cloud Services

The need for cloud services is usually driven by an organization's business units. Sometimes the process does not involve the CISO or even the CIO in the considerations for consuming cloud services and in the implementation process.

This chapter reviews the considerations that a CISO and a CCO, if existing in the organization, must take into account when preparing to construct a security plan when the organization intends to purchase cloud services.

This chapter refers to the model in which the responsibility is shared by the cloud provider and the organization (client) based on the models of service, deployment, and architecture for using the cloud.

Stage 1.1: Mapping Assets and Information Gathering

At this stage, the CISO must study and analyze the data relevant to cloud services in the organization.

1. The CISO must be familiar with the organization's business need behind the intention to purchase cloud services (excluding cases in which the consideration of purchasing cloud services is actually based on a need to heighten organizational security and protection).
2. It is appropriate to examine the issue of data security from the viewpoint of an organization operating in Israel. The CISO must examine the essence of the data the organization seeks to develop, use, and/or store via cloud services while considering the following aspects:
 - 2.1 **Laws or regulations** binding on the organization (e.g. **ILITA [Israeli Law, Information, and Technology Authority]** Regulations on Privacy Protection) that may forbid or limit the use of information in the context of cloud services altogether (e.g. due to security classifications, business sensitivity, or privacy protection issues), in particular data storage outside of Israel's borders.
 - 2.2 **Critical nature of availability** of information for the organization's ability to function, including that of its clients and providers and especially in the case of a system **whose activity is critical** to the Israeli economy, in the event of damage to a communications infrastructure connecting Israel to other countries.
 - 2.3 Will **exposure** of the data to unauthorized personnel **affect** the organization's ability to function, including that of its clients and providers?
 - 2.4 Will **damage to the credibility** of the data **affect** the organization's ability to function, including that of its clients and providers?
 - 2.5 Is the **level of protection** of the data in the cloud services **enhanced** compared to the level that existed before?
3. If possible, it is best to segment and define the sensitive elements of the information (e.g. credit card numbers, ID numbers).

4. The CISO must determine if the use of cloud services includes any operational aspect that, if damaged, will immediately and/or in an ongoing manner affect the operations of the organization's core business (e.g. **an organization whose main business is sales through a website stored by cloud services, where damage to availability would harm the organization's core business**).
5. The CISO must know what type of cloud service the organization plans to purchase (SaaS, PaaS, IaaS).
6. The CISO must know the cloud provider's basic information with regard to:
 - 6.1 Whether the provider is well-known and a leader in its field.
 - 6.2 Whether the provider meets well-known cloud service security standards set out by organizations such as CSA, HIPPA, ISO, PCI, FedRAMP, Nist, etc.
7. It is necessary to draft a **shared responsibility model** based on the type of cloud service and its deployment. Responsibility models may differ from one provider to another.
8. It is important that the definitions of the responsibilities for the operation, installations, maintenance, and protection of every layer are clear and documented in a **contractual document** when the agreement is drawn up.
9. The **layers** that must be addressed in a contractual agreement between a cloud provider and a client, **while clearly stating which of the parties bears responsibility for the operation and protection aspects**, are:

Layer	Explanation
Information	The type and the content of data that will be used and that can be accessed in the service under discussion.
User interface	The way the client or whoever needs to will access data.
Applications	The applications by which users' access to and use of data is made possible.
Database	Database for storing the data and applications.
Software	The codes used to develop and run applications.
Operating systems	The platform managing the hardware and software resources.
Virtual machines	An emulation environment the client will use.
Virtual network interface	The means and definitions of communications between virtual machines in the emulation environment.
Hypervisor	The software and interface to manage an emulation environment and virtual machines.
Hardware	The physical resources, such as processing power and memory, allocated to a client's use.
Storage	The physical resources allocated to a client for saving and storing data.
Communications	The mediation and method that allows access between the client's environment and the cloud provider's environment.
Physical location	The place where the cloud provider's physical resources used by the client are located.

10. vBreakdown of shared responsibility according to service model:

10.1 **IaaS:** Usually, the client is in control of and is responsible for many layers, from the virtual network interface level to the data.

Provider responsibility in IaaS model	Organization's responsibility in IaaS model
• Providing computing power based on what the client requires and has purchased. • Availability of computing resources throughout the contact period.	• Establishing the infrastructure, including: storage system, server system, and intra-organizations communications definitions. • User definitions. • Application and availability to users. • Application development, operation, and software licensing. • Protection of stored data (encryption, de-identification, etc.). • Business continuity.

10.2 **PaaS:** Usually, the client is in control of and is responsible for the applications layers.

Provider responsibility in PaaS model	Organization's responsibility in PaaS model
• Providing computing power based on what the client requires and has purchased. • Availability of computing resources throughout the contract period. • Supplying a platform for applications development and maintaining it, both in its different versions and in terms of patches (i.e. updates).	• Establishing intra-organizations communications definitions. • User definitions. • Application and availability to users. • Application development, operation, and software licensing. • Protection of stored information (encryption, de-identification, etc.). • Business continuity.

10.3 **SaaS:** Usually, the client does not have control or responsibility, except for the data type and content and the user interface definitions; otherwise, the responsibility lies entirely with the provider.

Provider responsibility in SaaS model	Organization's responsibility in SaaS model
- Establishing the infrastructure, including: storage system, server system and intra-organizations communications definitions. - Application and availability to users. - Application development, operation, and software licensing. - Protection of stored data. - Data encryption, if needed. - Business continuity.	- Information accuracy. - User definitions. - Data de-identification.

11. **An example** of a model of responsibility shared by the cloud provider and client by division into layers (as presented in the PCI Standard).

Cloud provider Client

Service model			Layer
IaaS	PaaS	SaaS	
			Data
			User interface
			Application
			Database
			Software
			Operating systems
			Virtual machines
			Virtual network interfaces
			Hypervisor
			Hardware
			Storage
			Communications
			Physical location

12. As previously noted, it is crucial to establish a **shared responsibility model** between the organization (client) and the cloud provider. However, this does not exempt the CISO from being familiar with the process-related and technical details and characteristics of each and every layer described in the previous section.

Even with regard to the layers which are contractually within the cloud provider's realm of responsibility, when, in the course of developing the organization's security plan, the CISO must refer to the cloud-related activities and services used by the organization, he or she needs to be familiar with and refer to each of the layers and ask the following questions:

- 12.1 **What controls are needed and appropriate for each layer?**
- 12.2 **What existing controls are there?**
- 12.3 **Is it possible to maintain them by asking the provider to supply them or will this need to be done by the organization, depending on the shared responsibility model?**
- 12.4 **If not, are there compensatory controls that may be maintained?**
- 12.5 **If not, is the risk of not maintaining these controls proportional?**
- 12.6 What is the layer's geographical location, its **physical location**? In terms of the organization's access, legal authority, potential sanctions for political reasons because the organization (client) is Israeli.
- 12.7 Which of the cloud services are the provider's own in-house services and which does the provider purchase from a sub-provider? Who is the sub-provider?
- 12.8 In this case, too, it is best to segment by **layers**. This will help the CISO know what products the organization is purchasing as part of its cloud service package in terms of hardware, communications, software, and applications. He or she can thus analyze the known risks and weaknesses of each of the products in the planning stage as well as later during the term of the service contract, and accordingly choose appropriate controls and responses.
- 12.9 The CISO should be familiar with past events such as attacks that may be associated with the cloud service provider and/or its sub-providers, with regard to the services supplied to the organization.

Stage 1.2: Risk Assessment

At this point, the CISO must identify the risks the cloud service poses to the organization based on the information gathered and analyzed.

- 13. The CISO must collate all relevant scenarios of damage to the organization resulting from the use of cloud services.
- 14. The CISO must know and refer to the deployment and architecture for using the planned and/or existing cloud according to the service model that is to be purchased.
- 15. As part of the scenario construction, it is best first to select **the threat**, i.e. the relevant final damage corresponding to the service model and cloud deployment.

For example: The CISO's analysis showed that **"The data stored in DB as part of the cloud services includes a list of clients' shipping addresses. Changes to those fields and damage to the reliability of the data are liable to cause the organization a great deal of operational and monetary damage. Therefore the CISO must analyze the scenarios in which changes to fields might occur."**

16. At the next stage, the CISO will have **to assess** the probability of each scenario actually occurring while taking into account existing control methods, in order to examine the need for additional controls, with respect to the following parameters:
 - 16.1 The level of expertise and resources needed to enable the scenario.
 - 16.2 The level of vulnerability of the relevant components which would enable the scenario.
 - 16.3 The level of logical access to the asset, given the service model, deployments, and architecture for using the cloud.
 - 16.4 The level of physical access to the asset, given the service model, deployment, and architecture for using the cloud.
17. After selecting the scenarios for all relevant final damage, the CISO must consider, in descending order of preference – from the most to the least likely scenario – the controls that must be applied and whether or not they can, in fact, be applied. If not, what operational alternatives are there, both from a business perspective and with reference to the service model, deployment, and architecture for using the cloud, which can provide a response that meets a reasonable level of risk management?

18. To return to the example of “Changes to those fields and damage to the reliability of the data are liable to cause the organization a great deal of operational and monetary damage,” then an example of this method of risk analysis would look like this:

The threat	Damage to data reliability: changes to data in lists of client addresses stored in DB server		
Cloud service model	IaaS		
Cloud deployment	Public		
Architecture for using the cloud	Multi-tenant		
Scenario	Probability analysis	Probability assessment	Controls to consider
A different tenant gains access to the list	• Level of specialization and resources – low • Level of DB server’s vulnerability – average • Level of other tenant’s logical accessibility – average • Level of physical accessibility – low	Average	• Encryption: separation by strong encryption with separate key management handled by the organization rather than the cloud provider. • VPC (virtual private cloud): virtual segmentation of environments by creating a private cloud inside the public cloud. • Separating tenants: separation by using separate physical components.

Chapter 2: Security Controls for Cloud Services

This chapter breaks down and provides examples of emphases for relevant security controls for a CISO to use when designing a security plan for cloud services in an organization.

2.1 Cloud Access Security Brokers (CASBs)

CASBs are security and control systems, some of which are sold by the cloud provider and others by third-party companies. They are located between the client and the cloud provider to allow integration or separation according to the organization's (client's) security definitions during the client's access to and use of cloud applications and services. They provide a response to the risks cloud services entail, enforce security policies, and meet regulatory requirements, even when the cloud services are external to the client's site and out of the client's direct control.

The features and capabilities of CASB systems are:

1. **Exposure:** Providing the client with the ability to see and control authorized and unauthorized services, allow control of cyber security and/or the client's IT instead of completely blocking certain cloud services, manage and limit access to activity and data within the services by division into user and/or machine permissions.

Exposure of unseen IT activity (shadow IT) in the form of applications, usage, users, data, and files in the cloud environment and third-party applications connected to the cloud, including mobile devices and synchronized clients.

2. **Compliance:** Providing the option to check if regulatory requirements applicable to the organization are being met to save and secure protection and privacy of client information, check applications and their use vis-à-vis relevant regulatory requirements applicable to the organization, and, when identifying gaps, provide the ability to perform changes and/or preventive actions to meet such requirements.
3. **Data protection:** Using a security application in the cloud consisting of a mechanism to identify and prevent data leaks, such as arranging fingerprints for documents in combination with contexts (user, location, activity, etc.). Managing permissions, sharing information, and generating tailor-made reports and warnings, as well as using encryption to transfer data.
4. **Threat protection:** The ability to scan, detect, handle, and block malicious and/or unauthorized activity in authorized and unauthorized cloud services by using malware analysis either statically or dynamically, identify user anomalies and prioritize handling of incidents based on severity.

2.2 Receiving Cloud Services from Several Providers Concurrently

1. Sometimes, organizations choose to or are forced to use cloud services from several providers, whether because of cost considerations or due to changes in the required applications, and even due to a security policy of risk separation and distribution.
2. Synchronization of providers is a challenge. Some provide IT operations services and others offer services related to data protection.

3. There is a lack of control systems that meet the standards to serve as APIs (application program interfaces) among the cloud services supplied by various providers. It is therefore possible to make use of open source software or cloud service management by a third-party provider to manage concentrated control with the capacity to monitor applications and servers, control access, and enforce policy.
4. Not all cloud providers offer the same services with emphasis on messaging tools, work flow, and management, and this may at times impose work at the lowest common denominator. A solution to this may be use of third-party software, usually open source , allowing alternate service suitable to the environments of all cloud providers.
5. Even when it comes to using similar, standard services, there may be differences among cloud providers in terms of how the same service is managed. In such cases, too, there are third-party providers who supply APIs specifically adapted for use among the various cloud providers.

2.3 Security Controls for Organizations Using Cloud Services

Control emphases refer to the unique aspects of cloud services. This is an expansion of the chapter on the control a CISO must implement in an organization's full security plan as described by **the Cyber Defense Methodology for an Organization** published by the National Cyber Security Authority. (The "Identify" column refers to identifying the control in the Cyber Defense Methodology for an Organization in the most immediate context, if it exists.)

IDENTIFY			
Family	Identification	Control	Example of control application
Responsibility of Board of Directors and management Compatibility	3.1 3.2	Ensuring there are effective processes relating to risk management policy and standards compliance	1. An organizational data protection and cyber security policy in terms of the organization's cloud services set up by management and the cloud provider; threats, scenarios, and controls to prevent them, DR & BC procedures, and incident identification and response processes. 2. Certifications that the cloud provider meets relevant standards to secure its services, such as: a. The cornerstones are ISO 27001, a standard issued by the International Standardization Organization that defines the principles of establishing, managing, and maintaining data security systems suitable to organizations, and SOC 2, a standard formulated by AICPA, the American Institute of CPAs, which tests security controls for maintaining data availability, reliability, and confidentiality in organizations. b. CSA STAR: Certification considered a leader in the field; comes in three levels. The second is based on maintaining ISO 27001 and the best practice matrix called CCM. c. ISO 27017/27018: Standards issued by the International Standardization Organization defining security controls and privacy in cloud services. d. PCI-DSS (Payment Card Industry Data Security Standard): Standard issued by credit card companies to protect credit data and transactions A document called Cloud Computing Guidelines. e. NIST-SP 800-144: Security controls for cloud services issued by the National Institute of Standards and Technology that federal organizations in the United States are required to implement as part of FISMA (the Federal Information Security Modernization Act) to get an operator license. f. FedRAMP (Federal Risk and Authorization Management Program): A federal US program of risk assessment, permissions and control of cloud services (relevant to company activity in the United States, especially vis-à-vis government bodies). g. ILITA (Israeli Law, Information, and Technology Authority): Privacy Protection Regulations 7809 defining database security. h. EU GDPR (General Data Protection Regulation): Privacy protection regulations issued by the EU. i. HIPAA: Law applicable in the United States primarily aimed at protecting privacy and securing confidential medical data.

IDENTIFY			
Family	Identification	Control	Example of control application
Compatibility		Enforcement of private policy	3. A legal agreement involving the client's legal counsel, which clearly defines the cloud provider's responsibility for data protection allowing personal identification, and including reference to compensation for damages and/or loss. 4. Getting the cloud provider to sign the privacy protection agreements of relevant regulators. 5. Separation of databases: data stored in cloud service containing anonymous lists and data revealing personal identification linked to anonymous lists should be stored on the client's premises or with the cloud provider in a more secure manner.
Control and audits	3.4	Audits of operational and business processes	6. Receiving audit reports from cloud provider, such audits executed by an independent third-party auditing institution of operational and business processes that are part of the services to understand security controls that the cloud provider applies as part of its services, with emphasis on the following issues: a. Security controls ensuring separation of client's applications and data from those of other clients in a multi-tenant environment. b. Security controls ensuring the prevention of unauthorized access by cloud provider workers to client data and applications (e.g. SOC 2). 7. Ensuring that there are also audits to provide security for self-service measures in addition to the services the cloud provider offers, such as a means of registering for the service or payment procedures. Such self-service client measures are usually more vulnerable than the service itself and it is therefore necessary to make sure that the audits include these as well.

PROTECTION			
Family	Identification	Control	Example of control application
Supply chain and outsourcing	16.2	Using legal and contractual tools to define the responsibilities of cloud provider and client	8. A binding service contract specifying the division of responsibility between the provider and the organization. It is possible to specify this at the level of the layers. Responsibility must refer to protection and security of the layer, to operations, and to handling mishaps. 9. A service contract must include the location of the data (physical, specifying the countries), the laws applicable to it and a commitment that the data will not be moved to a different jurisdiction without the client's knowledge. 10. The contract must also include a reference to every sub-provider providing services to the main cloud provider in the context of the cloud services provided. 11. The service contract must refer to the cloud provider's obligation to report to the client on network penetrations, the discovery of malware, mishaps, failures, and any type of incident that risks or affects the client's data and functional capacity in the context of the cloud services provided. 12. With regard to reporting, the contract must specify schedules, reporting procedures, the party responsible for the incident as part of setting indexes for indemnification and compensating the client if necessary. 13. An example of a service contract is presented by the (Cloud Security Alliance) (CSA): "Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union."

PROTECTION			
Family	Identification	Control	Example of control application
Access control HR	4.6 4.7 4.29 4.34 19.10	Management of personnel, functions, and identities	14. For clients whose organizations have a system of identity and permissions management, we recommend expanding its use in the context of access to cloud services, both from the point of view of efficiency and from the point of view of control of an employee's change of position or termination. 15. The client must have permissions to manage users' identities and permissions. 16. The client must characterize how synchronization occurs when a new user is established, with emphasis on temporary positions, changes to current users, and closing out users who leave. Mishaps in synchronization are liable to give rise to data exposure risks. 17. The ability to execute an entry and log-off of a user in a single process (AD federation) to ensure that the connection to all cloud services is terminated, acquiring IDaaS (Identity as a Service). 18. Audits and logs of access and use by users of cloud services, including identification of the user at login (user name, stations where the login was carried out, login failures, access or failure of access to compartmentalized areas), retrieval or removal of data such as printing, and more. 19. Support with complex, strong identification mechanisms, such as dual- or multi-stage identification, biometric identification, etc. 20. The client's ability to describe and enforce, in the context of accessing cloud services, management of function and groups in the organization based on the security policy under which it operates. 21. Limiting access based on positions, network addresses, MAC, and geographical location.

PROTECTION			
Family	Identification	Control	Example of control application
Data security	5.2 5.3 5.4 5.5	Segmenting and classifying data for the sake of implementing appropriate security	22. Creating a list of data assets: identifying the assets, classifying them in terms of their importance to the client and/or applicable regulation, defining the owners and their responsibility for issues related to data, data location, and access to it. 23. For all data types: a. Structured data (ERP, CRM) stored in databases in a multi-tenant environment: security by separation and isolation or mixing in the database, use of encryption to secure the database. b. Non-structured data (images, document scans, and multimedia files) may be sensitive and should be edited, or the data should be shielded (signatures, home addresses, and other personal data). 24. Relating to data privacy: based on the legal and regulatory requirements on access, storage, and use of data allowing personal identification. Setting up limits on access and use of data, marking the data as such, storing in a secure manner with reference, for example, to geographical location, and providing access only to authorized users. 25. Implementing data confidentiality, reliability, and availability: using applications that can classify data, encrypting sensitive data in storage and transmission, and, in relation to separate storage of encryption keys, using data verification techniques such as hashing, using backups and quick recovery applications. 26. Applying identification and data access permission mechanisms and gathering history and logs of access and use for the purpose of audits and investigations. 27. Monitoring data transfer actions between client and cloud provider in order to reduce/prevent unauthorized data transfers by means of: a. DAM – database activity monitoring b. FAM – file activity monitoring c. URL filtering d. DLP – data loss prevention 28. Using IDA mechanisms by which data is split into several pieces, each piece being stored in a different storage server. 29. In the IaaS model: encrypting volumes to protect against duplication and unauthorized access.

PROTECTION			
Family	Identification	Control	Example of control application
Network security Preventing malicious code Separating environments	7.1	Filtering, identifying and separating for protecting network traffic	30. Filtering network traffic using applications such as firewalls, if there is a firewall service managed by the provider (usually managed by the client). a. Requiring the cloud provider to give a list of open ports. b. With regard to filtering network traffic, also using the IPv6 protocol, not only the IPv4 protocol. 31. Protection against distributed denial of service (DDOS) attacks: the cloud provider's and its internet provider's ability to handle high-volume network traffic, such as identifying a large-scale attack on the provider, identifying a small-scale attack focused on the client's server, automatic warnings of an attack, use of WAFs (web application firewalls), the ability to carry out a post-attack analysis. 32. Using up-to-date scanning software to protect against malware, provided by the cloud provider or by third-party software with API suited to the provider's services: a. At the level of the operating system of the end stations and servers: up-to-date, continuously-managed anti-virus. In SaaS and PaaS models, this is the provider's responsibility; in the IaaS, it is the client's responsibility. b. Filtering communications traffic: use of IDS/IPS systems, WAF; in all models this is the provider's responsibility. c. Filtering traffic, receiving files in emails and browsing: SandBox MailRelay. SaaS and PaaS – provider's responsibility; IaaS – client's responsibility. d. Browsing: filtering using URL filtering and proxy; in all models – provider's responsibility.
	7.6		
	9.3		
	9.9		
	9.24		
	10.2		
	10.8		
	10.9		

PROTECTION			
Family	Identification	Control	Example of control application
Network security Preventing malicious code Separating environments	7.1	Filtering, identifying and separating for protecting network traffic	33. Logs and updates: a. Receiving the ability from the cloud provider to view the intactness of the network via a system or interface, in real time. b. Clarification on scenarios for handling incidents (such as attacks) and procedure for reporting to client: defining the types of incidents the cloud provider must report to the client, such as the identification of malicious code in the client's server or identification of malicious communications from client's server to attacker's server (C&C), how the incident is handled, help in assessing damage and actions to fix and secure the system to prevent recurrence. c. Relating to legal limitations on collecting and storing logs in terms of privacy protection. d. Client to define for the cloud provider which logs and how it may receive them for the purpose of an independent investigation of incidents. 34. Tools and means for separating clients from one another and clients from the internet: a. Network segmentation by means of virtual network separation (VLANs). b. Encrypted traffic: connecting to site-to-site or client-to-site service by VPN (virtual private network), use of encryption such as IPsec, TLS/SSL. c. Firewall to filter traffic between VLANs. d. The provider to filter network traffic, e.g. by using Hypervisor or ebtables (Linux software for filtering network traffic). 35. Hardening virtual machines and servers, such as blocking and canceling services, using patch management systems to update security patches; in SaaS and PaaS model – provider's responsibility, in IaaS model – client's responsibility. 36. Protecting the cloud provider's internal network: the client must ensure that the cloud provider applies security audits of its own internal network, shows the findings of third-party audit reports, or has proof of meeting relevant regulatory standards.
	7.6		
	9.3		
	9.9		
	9.24		
	10.2		
	10.8		
	10.9		

PROTECTION			
Family	Identification	Control	Example of control application
Physical and environmental security	18.8	Security audits of physical means and sites	37. Analyzing existing risks of the physical, geographical location where the cloud provider stores the data, with reference to natural disasters, crime level, and level of social and/or political unrest.
	18.15		38. Application of filtering audits and prevention of physical access by unauthorized personnel to cloud provider's sites and locations that store means and infrastructures serving the client in the context of cloud services: a defined site, guards, electronic entrance control, camera monitoring, electronic alarms, etc.
	18.17		
	18.19		
	18.20		
			39. Application of prevention controls and damage reduction means subsequent to external or environmental events: extreme weather, flooding, fire, earthquake, electrical outage, and others. For example, proof of meeting Israeli Standard 1243 "Fire Safety of Computers and Peripheral Equipment" or ISO 27001, which defines, e.g., fire suppression with gas in server rooms and electricity panels, temperature sensors, drainage solutions, Uninterruptible Power Supply (UPS) and/or generator, etc.
			40. Application of controls against theft, loss, malicious damage, and vandalism of means and infrastructures relevant to cloud providers: electronic entrance controls, guards, camera monitoring, electronic alarms, locks, etc.
			41. Preventive controls against data loss and/or leakage in case of discarding or reuse of data storage equipment: inventory management, use of companies that scrap and shred electronic equipment and magnetic media, deep wipes of non-volatile memories.

DETECT			
Family	Identification	Control	Example of control application
Documenting and monitoring	21.4 21.5 21.12	Receiving warnings and reports from cloud provider	42.Client access to warnings by the cloud provider's security control systems, e.g. SEIM, with respect to the identification of suspicion of a malicious incident. 43.Receiving reports from the cloud provider of every incident that posed a risk of damage to client's assets, including logs allowing forensic analysis of the incident; • identity of the system whose sensor reported to SEIM, the SEIM rule based on which a warning was issued, • testing and analysis to verify or find the source of the alarm, • fixes to prevent a recurrence, etc. 44.Receiving analytical reports from the cloud provider pertaining to verification, permissions, and data management with regard to applications and data used by client vis-à-vis security controls that the cloud provider applies.

RESPOND			
Family	Identification	Control	Example of control application
Incident management and reporting	24.3	Articulating an incident response plan with the provider	45. Ensuring that the service provider has an incident response service covering the following: a. Incident identification: how incidents are identified, whether there is 24/7 monitoring, if the analysis of the identification is done by an analyst or by automated technological means. b. Specialized personnel to handle incidents: the provider declares the level of professional knowledge of its personnel and the personnel's attitude to the number of incidents and the provider's clients. c. Analysis and deep search to detect the party responsible for the incident and application of actions to prevent recurrence: whether there is an orderly methodology, impressions from reports summarizing previous incidents handled by the provider. 46. In writing, determining the manner, schedules, and types of incidents for issuing an incident report to the client: e.g., receiving a report of an incident in which one or more of the CIAs (confidentiality, integrity, availability) was affected, leakage, disruption, or accessibility of data and services relevant to client; how the provider handles a suspicion of an incident in which the suspicion was not refuted within 24 hours, etc. 47. In writing, determining the manner, stage, and type of incident to share with the client's response team in order to handle an incident: based on the client's ability to provide a response team and the provider's willingness to allow it. This is relevant in particular to the IaaS model.

RECOVER			
Family	Identification	Control	Example of control application
Business continuity	25.1	Implementing backup and recovery plans by the cloud provider in case of a mishap or damage	48.Ensuring that the cloud provider has a business continuity plan <u>in writing</u> (BCP=business continuity planning) and the company's recovery from a disaster (DRP=disaster recovery plan) and <u>whether or not it has been drilled</u>. 49.Ensuring the provider has a DR site where hot backups (in real time) and/or cold backups (regularly scheduled) are carried out based on the definition of the necessary and critical nature of the data for the client. 50.Checking the physical location of the DR and examining whether there are, at the site, regulatory limitations or governmental danger or risks associated with the nation's political and security status liable to affect the availability and operational status of the site. 51.Drawing up an SLA (service level agreement) to receive service, to go on-air to reconstruct backups: based on client analysis of the critical nature of service availability or data (in minutes, hours, days); prioritize with the provider based on the provider's fees and technical capacity.
	25.10		
	25.14		
	25.17		
	25.19		

RECOVER			
Family	Identification	Control	Example of control application
	11.2	Defining the process of ending the service	52. In the contract, defining the notice period both parties must allow for ending the relationship, usually 30 days. 53. The client must have a previous plan for how and what he needs to transfer the data or service (in case continued service is necessary) to another cloud provider, within the notice time. 54. It is necessary to define, ahead of time and with the provider, a secure way to transfer the data stored with the cloud provider to the client at the end of the contract, based on the client's needs and requests, e.g., physical transfer of storage means or using encrypted communications, based on the data amount and type. 55. The contract should stipulate that the cloud provider is obliged to save, for a period of one to three months, the client's data to ensure that the copy transmitted to the client is usable and free of corruption. 56. It is necessary to stipulate that wiping the data will occur only after receiving the client's written permission rather than unilaterally by the provider. 57. In general, it is necessary to define ahead of time with the cloud provider the manner in which data, backups, logs, and audit reports will be wiped when the contract ends in a way that ensures that the client's data cannot be restored and there is no risk it will leak to an unauthorized party, using deep wipe, and relisting data on the storage disk. 58. Receiving an official written declaration from the provider that the data has been wiped using a mechanism previously decided on together with the client.



The Prime Minister's Office
National Cyber Directorate
National Cyber Security Authority

