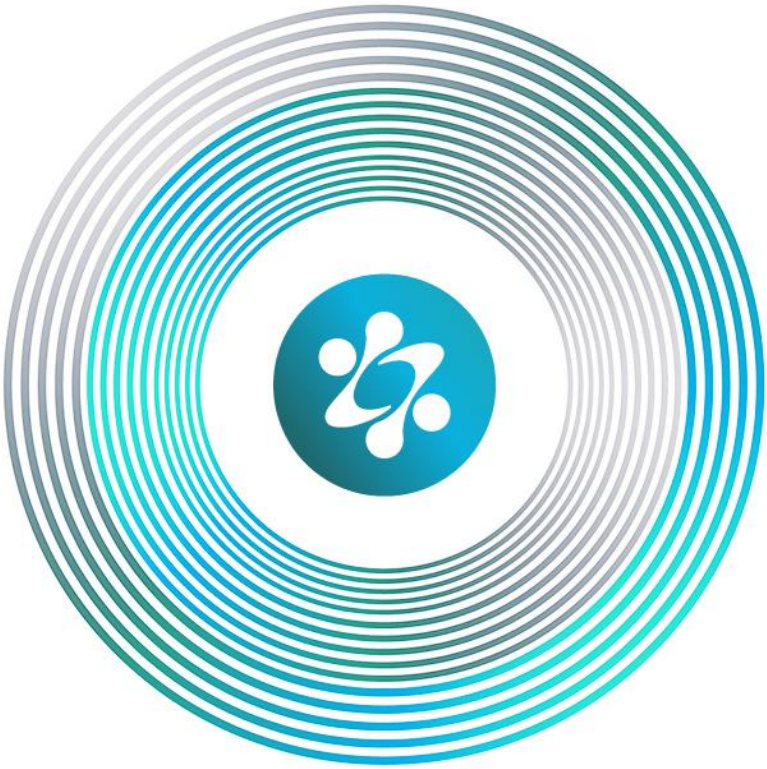


Public Cloud Security

with a Focus on Ransomware

Version 1.01

Unclassified, TLP:CLEAR

December 05, 2024

Contents

Terms of Use

The information is provided as is; use thereof is the user's responsibility, and may require a cyber defense professional, acquaintance with the organization's systems and fine-tuning to its characteristics.

Comments and remarks regarding this document can be emailed to the Defense Division at: 119@cyber.gov.il

Executive Summary

An analysis of cyber incidents with respect to the last five years found that ransomware attacks were behind 32% of cyber incidents, and responsible for 38% of financial losses. In 2015, ransomware incidents constituted just 1% of cyber incidents, but grew sharply in recent years to constitute a significant 52% of cyber incidents in 2023.

A typical ransomware incident incurs costs amounting to $1.4 million! That is more than 12 times the average financial damage caused by other cyber attacks. Severe ransomware incidents are likely to be much more destructive. In extreme cases, damage can add up to as much as $50 million, compared to $22 million for cyber attacks not involving ransomware. [1]

Attempted attacks against public cloud services, including ransomware attacks, have risen in recent months and years as part of a global trend to exploit organizations that use cloud services to store their infrastructures and data. **Most successful attacks are due to misconfigurations and flawed and/or less than optimal implementation by the Cloud Service Customer (CSC), exposing attack vectors and vulnerabilities to be exploited. Usually, without the need for a high level of expertise and\or investment of major resources[2] on the part of the attackers.** [3]

One of the "pinnacle" events of 2023 was the attack on a Cloud Service Provider (CSP), which used a product called MOVEit that contained a vulnerability, paving the way for an attacker to perpetrate a ransomware attack. This highlights the fact that the ransomware threat is also a very pertinent threat to organizations that consume public cloud services. [4][5]

[1] Information Risk Insights Study RANSOMWARE, Cyentia Institute, 2024
A Detailed Analysis of the Frequency and Impact of Ransomware Events
https://www.cyentia.com/iris-ransomware/
[2]Note that this document uses both the terms "asset" and "resource", which refer to the same thing.
[3] Top Threats to Cloud Computing 2024, CSA, August 05, 2024
https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024
[4] MOVEit Exploit & Ransomware Attack: Why SaaS Security Is Critical During a Cyberattack
https://cloudsecurityalliance.org/blog/2023/11/08/moveit-exploit-ransomware-attack-why-saas-security-is-critical-during-a-cyberattack
[5] MOVEit Vulnerability Weaponized in Ransomware Attack
https://blog.checkpoint.com/security/moveit-vulnerability-weaponized-in-ransomware-attack/

According to an Israel National Cyber Directorate report, cyber attacks cost Israel NIS 12 billion annually.[6] If organizations and individuals in the Israeli economy don't take appropriate defensive actions, these costs are expected to continue growing annually in the coming years as technology permeates all areas of our lives, and given the expected increase in the quantity and quality of the attacks.

The purpose of this document is to provide compiled information aimed at cyber information and defense units on the following issues:

1. Cyber threats in general, and the ransomware threat in particular, and their potential impact on organizations that use public cloud services.
2. Case studies in order to promote awareness about the ransomware threat: readers can also use the case studies and other relevant information in discussions before steering committees and decision-makers, and in planning and implementing defensive actions.
3. Ways of mitigating risk so that organizations can adopt the recommendations and adapt their annual security plan for contending with ransomware attacks.

Note that in reviewing the aforementioned issues, and document also provides pointers to other sources of information.

[6] Cyber attacks in Israel cost the country NIS 12 billion a year, the Israel National Cyber Directorate, April 2024 https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_5_2024

Introduction

General background

Cloud computing is an operating model and a set of technologies used to manage shared IT resources by abstracting the computing, network, storage, etc. The cloud model vision presents a reality in which components and resources can be rapidly orchestrated, allocated and deployed, and resources scaled up or down as necessary, and even removed, enabling a dynamic model of consumption and deployment.

The benefits include collaboration between stakeholders, agility, flexibility, availability, and reduced costs. Also, accessibility to new technologies not routinely available to organizations with limited resources.

The global trend is to transition to using a public cloud

There has been a clear and growing trend in recent years whereby more and more organizations have transferred management of their resources and data to public cloud services. This transition is reflected in the external storage of the organization's data and/or in the external management of IT resources. According to estimates,[7] the volume of data stored in cloud services will reach around 200 Zettabytes by the end of 2024[8].

There are dozens of companies providing cloud services to customers of different sizes, small and large, for different purposes, from websites to huge projects stored and run completely with the aid of cloud resources. Among the cloud services providers, three veteran providers command two thirds of market share: AWS (Amazon Web Services), part of Amazon and one of the oldest in the field, commands a 31% market share; Azure, the service established by Microsoft in 2010 commands a 24% market share; and GCP (Google Cloud Platform), the cloud provider under parent holding company Alphabet, commands an 11% market share.

[7] The World Will Store 200 Zettabytes Of Data By 2025
https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025
[8] A Zettabyte (or ZB) is equivalent to 10^{21} (1,000,000,000,000,000,000,000) bytes or one trillion gigabytes

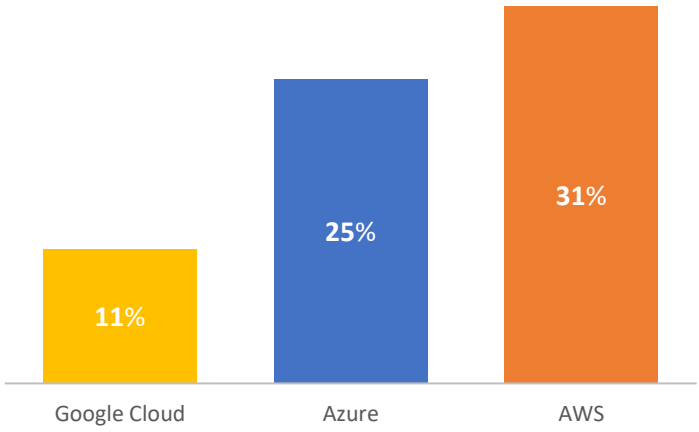


Figure 1: The scale of use of the well-known giant providers, as at Q1 2024[9]

The transition to use of the public cloud has attracted not only customers and organizations, but as with many technological trends, also attracted bad actors that seek to exploit these platforms. It therefore comes as no surprise that with increased use of public cloud services, more and more ransomware campaigns by bad actors against organizations using these platforms have been identified.

An analysis of cyber incidents over the past five years found that ransomware attacks were behind 32% of cyber incidents, and responsible for 38% of financial losses. In 2015, ransomware events constituted just 1% of cyber events, but grew sharply in recent years, comprising a significant 52% of cyber incidents in 2023. A typical ransomware incident incurs costs of $1.4 million! That is more than 12 times the average financial damage caused by other cyber attacks. Severe ransomware incidents are likely to be much more destructive. In extreme cases, damage can add up to as much as $50 million, compared to $22 million for cyber attacks not involving ransomware. [10] Attempted attacks against public cloud services, including

[9] Amazon Maintains Cloud Lead as Microsoft Edges Closer
https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers

[10] Information Risk Insights Study RANSOMWARE, Cyentia Institute, 2024
A Detailed Analysis of the Frequency and Impact of Ransomware Events
https://www.cyentia.com/iris-ransomware/

ransomware attacks, have risen in recent months and years as part of a global trend to exploit organizations that use cloud services for storing their infrastructures and data. Most of the successful attacks are due to misconfigurations and flawed and/or less than optimal implementation on the part of the Cloud Service Customer (CSC), exposing attack vectors and vulnerabilities to be exploited. And this, generally, without the need for great expertise and/or investment of extensive resources on the part of the attackers. [11]

One of the "pinnacle" events of 2023 was the attack on a Cloud Service Provider (CSP), which used a product called MOVEit that contained a vulnerability, paving the way for an attacker to perpetrate a ransomware attack. This highlights that the ransomware threat is also a very pertinent threat to organizations that consume public cloud services. [12][13].

According to an Israel National Cyber Directorate report, cyber attacks cost Israel NIS 12 billion annually.[14] If organizations and individuals in the Israeli economy don't take appropriate defensive measures, these costs are expected to continue to grow annually in the coming years as technology permeates all areas of our lives and the quantity and quality of the attacks increase.

Given these facts, organizations that use public cloud services need to take appropriate steps to mitigate the risk of cyber incidents, including ransomware attacks, which can cause both direct and indirect damage.

[11] Top Threats to Cloud Computing 2024, CSA, August 05, 2024
https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024
[12] MOVEit Exploit & Ransomware Attack: Why SaaS Security Is Critical During a Cyberattack
https://cloudsecurityalliance.org/blog/2023/11/08/moveit-exploit-ransomware-attack-why-saas-security-is-critical-during-a-cyberattack
[13] MOVEit Vulnerability Weaponized in Ransomware Attack
https://blog.checkpoint.com/security/moveit-vulnerability-weaponized-in-ransomware-attack/
[14] Cyber attacks in Israel cost the country NIS 12 billion a year, the Israel National Cyber Directorate, April 2024
https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_5_2024

Standard cloud deployment models

There are generally regarded to be four cloud deployment models:[15]

1. **Public cloud -** cloud services are provided by means of shared infrastructure (hardware, software and utilities) open to all, sometimes free of charge. While logical, and sometimes physical, division and separation of customers and accounts exists, resources are shared.
2. **Private cloud -** cloud services are provided by means of infrastructure (hardware, software and utilities) accessible only to one specific customer. Sometimes this infrastructure is located on-premises organizational infrastructure at the customer, and sometimes on the cloud provider site. The communication and access to the infrastructure are given exclusively to the designated customer, who may be highly involved in managing it.
3. **Community cloud -** a specific sector or multiple organizations with a shared interest come together to be provisioned cloud services dedicated specifically to them.
4. **Hybrid cloud -** a customer uses a private cloud for specific applications, as well as a public cloud to link the data or the application to other applications or data.

In cloud computing, the architecture can be implemented in one of two formats:

- **Single-Tenant** - according to the type of cloud service and deployment, the CSC is the only entity that uses the resources. The aforesaid may be extend from use of a hardware resource to an application developed specifically for the CSC (mostly in a private cloud).
- **Multi-Tenant** - in this case, according to the type of cloud service and deployment, one CSC shares resources with one or more CSCs. In other words, the level of isolation is lower than in a single-tenant scenario.

[15] NIST SP 800-145 - The NIST Definition of Cloud Computing, NIST, September, 2011 https://csrc.nist.gov/pubs/sp/800/145/final

Typical models of public cloud services

Several typical models of public cloud services exist, the most notable ones being[16]:

- **Infrastructure as a Service (IaaS) -** the basic and most common model, as a service to companies and organizations. Its main aim is to avoid the need to build data centers and to purchase and maintain hardware components, including storage arrays, servers, communications components and information security components, and instead to pay for services according to consumption using a model of virtual objects that can be controlled via a service interface.
- **Platform as a Service (PaaS) -** according to this model, in addition to the hardware components and the infrastructure, the CSP provides the customer with a platform of basic software packages for the application development environment, and for customer product testing, and also provides IT services from within the platform.
- **Software as a Service (SaaS) -** according to this model, the CSP provides the hardware and the infrastructure, as well as the customer's end-user applications, where the application is purchased from a company that specializes in the relevant domain.

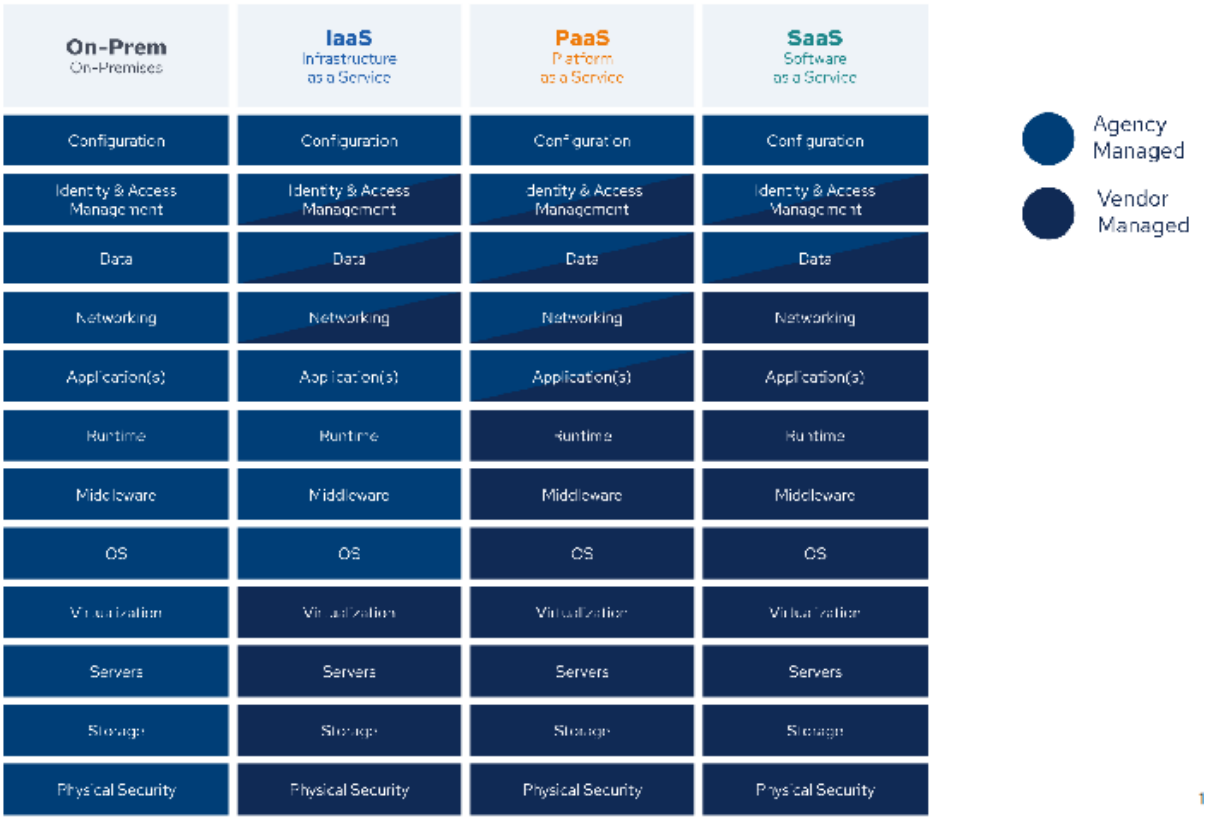
Shared Responsibility Model (SRM)

In most cases CSPs use a Shared Responsibility Model (SRM) to specify the role of each party to the contractual engagement agreement, and the security tasks under its responsibility.

However, in practice, the requirements of the Law and regulations don't absolve the CSC of its accountability in providing a suitable level of security for the data and services. Therefore, the CSC should view this model as a decision support tool only, and is fully responsible for the consequences of the risks and exposure incurred by entering into a contractual engagement with a CSP.

[16] NIST SP 800-145 - The NIST Definition of Cloud Computing, NIST, September, 2011 https://csrc.nist.gov/pubs/sp/800/145/final

The following figure presents a typical shared responsibility model:



17

Figure 2: A typical shared responsibility model

In general terms, the shared responsibilities can be divided according to the service model selected:

[17]The diagram is taken from the following document:
Security Guidance for Critical Areas of Focus in Cloud Computing v5, CSA, July 15, 2024
https://cloudsecurityalliance.org/artifacts/security-guidance-v5
which is based on the American CISA model of division of responsibilities

IaaS - in most cases, the CSC has control and responsibility for many layers - from the level of the virtual network interfaces to the level of the data:

The CSPs responsibility in an IaaS model	The CSCs responsibility in an IaaS model
• The provider is responsible for providing the computing power in accordance with that required and purchased • The provider is responsible for the availability of the computing resources throughout the period of the contractual engagement	• Setting up the infrastructure, including: the storage array, the array of servers, intra-organizational communications settings • Defining users and permissions • Responsibility for the application and its availability to the users. • Responsibility for developing the application, running it and for the software licenses • Responsibility for protecting the stored data (encryption, anonymization, etc.) • Responsibility for business continuity

Table 1: The division of responsibilities between the parties in an IaaS model

PaaS - in most cases, the CSC controls and bears responsibility for the application and utility layers and their availability to the users:

The CSPs responsibility in the PaaS model	The CSCs responsibility in the PaaS model
• The provider is responsible for providing the computing power in accordance with that required and purchased • The provider is responsible for the availability of the computing resources throughout the period of the contractual engagement • The provider will provide the platform for the development of applications and will be responsible for maintaining them in terms of file versioning and installing security patches	• Intra-organizational communications settings • Defining users and permissions • Responsibility for the application and its availability to the users • Responsibility for developing the application, running it and for the software licenses • Responsibility for protecting the stored data (encryption, anonymization, etc.) • Partial responsibility for business continuity (e.g. backups and validation)

Table 2: The division of responsibilities between the parties in the PaaS model

SaaS - in most cases, the CSC has very little control and very limited responsibility, apart from the data type and contents of the data and for user definitions and permissions; the responsibility, for the most part, falls on the CSP:

The CSPs responsibility in the SaaS model	The CSCs responsibility in the SaaS model
• Setting up the infrastructure, including: the storage array, the array of servers, intra-organizational communications settings • Responsibility for the application and its availability to the users. • Responsibility for developing the application, running it and for the software licenses • Responsibility for protecting the stored data • Responsibility for data encryption, as necessary • Responsibility for business continuity	• Responsibility for the correctness of the data • Defining of users and permissions • Responsibility for data anonymization • Partial responsibility for business continuity (e.g. backups and validation)

Table 3: The division of responsibilities between the parties in the SaaS model

Nesting cloud

A nesting cloud is a hierarchical work configuration in which one CSP utilizes the infrastructure of another CSP. For example: a CSP provides its customers with services on a SaaS basis, while relying on the core infrastructures of another CSP that provides

it with infrastructure on an IaaS basis. This work configuration enables a CSP with limited resources or other business need to have access to advanced capabilities not normally available to it.

However, this work configuration creates a high level of dependency between the CSPs, while CSCs, especially those that use SaaS, are often not aware of the dependency at all. This fact may impact the ability of the CSC to comply with the requirements and indicators of business continuity, as well as with other requirements, such as the need to maintain data sovereignty.

Typical interfaces for managing a public cloud environment

Cloud access is made possible through a number of typical interfaces. The security concept calls for the CSC to ensure that these interfaces are protected by an appropriate level of security. Misconfiguration or inadequate security controls for the risk level may give the attacker quick and convenient access to the organizational data.

Below is a review of typical management interfaces:

1. **Web management console**, which may include expansion modules, such as Cloud Shell and a bastion host. This interface generally also enables loading of files, such as a user accounts list, in order to simplify automation.
2. **CLI**, which is run from the user endpoint, and also enables full or partial automation.
3. **API**, which enables M2M and H2M connectivity, and provides advanced and extensive management capabilities. Including expansion of capabilities in order to execute integration with external products and services.
4. **SDK**, which enables software makers and others to expand the capabilities of their solution by integration with a public cloud environment. A common implementation includes use of an API that the public cloud provider externalizes.
5. **IMDS -** a service that enables access of an instance of a specific asset to its metadata. Despite the fact that it is considered an "internal" service that is not normally accessible to the end customer, misconfiguration of it could enable cyber attacks even beyond the CSCs cloud environment. Such as the use of SSRF.

6. **VPN -** an interface that enables a temporary or permanent remote connection between sites (S2S).

Over and above public cloud management interfaces, resources such as virtual machines and containers, may externalize management interfaces. Below are several common examples:

1. **RDP -** a common management interface in MS Windows.
2. **WS-Management/ WS Remoting -** an interface that enables remote running of Power Shell commands and scripts.
3. **WMI -** a Windows configuration settings management interface.
4. **SSH -** a common management interface in Linux.
5. **SNMP -** a common management interface for network devices, such as a FW.
6. **Third party remote access, management and monitoring (RMM) interfaces**
7. **Dedicated management protocols** for information security, cybersecurity and system security solutions.

Common techniques used by ransomware attackers

Ransomware in its original form is malware that seeks to prevent an individual or organization from accessing data by encrypting it, and demanding that the victim pay a ransom in order to release the data.

Several techniques have been developed by ransomware attackers in recent years:

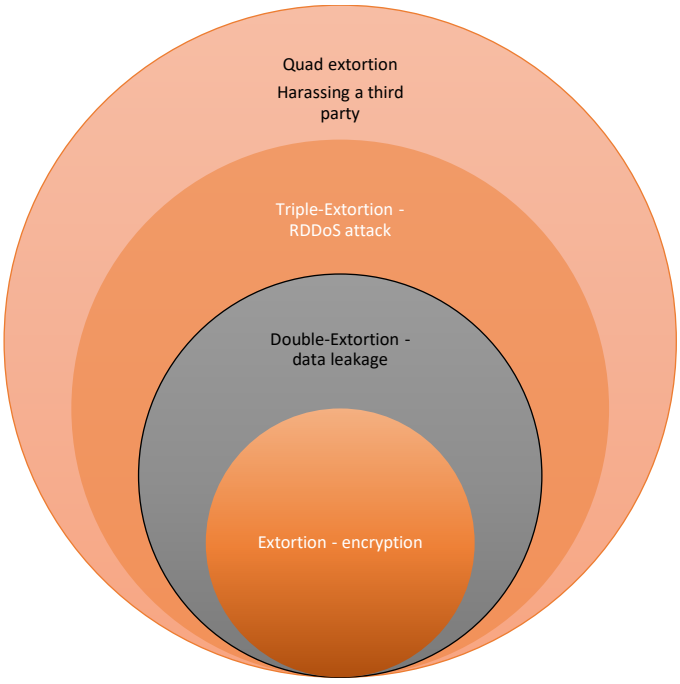


Figure 3: Common techniques used by ransomware attackers

That is, attackers' techniques have evolved over the years, with each new technique incorporating its predecessor and adding a new capability. Below is a more detailed description:

No.	Technique	Details
1.	Extortion - encryption	Prevents access to data by encrypting the data. The organization ("the victim") has to comply with the ransom demands as a precondition for removal of the encryption. This was the first technique used by ransomware attackers.
2.	Double-Extortion - data leakage	Leaking data before their encryption/ deletion, in order to widen the scope of the CSCs exposure. For example: the threat that exposure of sensitive data will harm the victim's reputation and/or result in regulatory sanctions being imposed.
3.	Triple-Extortion - RDDoS attack[18].	RDDoS attack.
4.	Quad-Extortion - harassing a related third party	Directly or indirectly threatening an end customer or other stakeholders (such as the regulator) in order to have them put pressure on the CSC to fulfill their demands or as punishment for their refusal to comply with the ransom demands.

Table 4: Common techniques used by ransomware attackers

To strengthen the impact of the attack, a combination of the following tactics is often employed:

[18] In a public cloud, this attack goes by the names: Denial-of-Wallet (DoW) and Economic Denial of Sustainability (EDoS)

1. **Data corruption -** the attacker modifies the existing data in order to compromise their trustworthiness and integrity**.** The data modification process often takes place over time (weeks/ months/ years), in order to make it difficult or even impossible for the CSC to detect the changes applied**.** This also enables the attacker to ”contaminate” the backups over the course of time, so that the CSCs restore process is rendered ineffective**.**
2. **WIPER -** prevents access to data by deleting the data**.** With emphasis on deleting of backups, snapshots/ file versioning and replications**.** The aim is to make it difficult or even impossible for the CSC to recover from the incident**.**
3. **Adding of ”background noise” -** the attacker may employ multiple attack vectors in parallel or serially in order to overwhelm the CSCs information security and cybersecurity team and/or to cover its tracks**.**

Case studies of cyber attacks against a public cloud environment

This section reviews several case studies of attacks on a public cloud environment in order to better acquaint information security and cybersecurity personnel with such attacks. The information in this section can be used to help mobilize decision-makers into promoting an organizational culture that is information security and cybersecurity driven.

Attacks on CSPs

CSP servers hit by a dependency confusion attack

Modern software generally includes libraries and modules (software packages) that originate outside the organization. The libraries are mostly concentrated in formal or semi-formal public code repositories. These software packages are also known as software dependencies because the software is dependent on the downloading of the packages and intact incorporation of them in the build process in order to function properly.

Well-known repositories exist for the different programming languages, such as: PyPI for Python, NPM for Node.js, RubyGems for Ruby, Maven for Java, and NuGet for .Net. Users, be they organizations or private individuals, can publish the code they developed, in these repositories.

These repositories do not generally have effective work practices for information security and cybersecurity, and therefore malicious code is often detected in them.

During the software build process (whether done manually by a developer or automatically using CI/CD processes), package manager software downloads the latest versions of the libraries in use to the developer endpoint or to a server, and the code is added to the proprietary code that was written by the developer or the organization.[19]

[19] Exploitation of Software Dependencies in Attacks, the Israel National Cyber Directorate, February 16, 2021 https://www.gov.il/he/pages/dependencies

The CSP allowed CSCs to define a URL to an external code repository, making the CSCs vulnerable to dependency confusion attacks. The attacker could execute the code remotely (RCE) on a managed workflow orchestration service called Cloud Composer. The specific CSPs vulnerability was exposed in 2024, while this type of vulnerability was already known of since 2021.[20]

A design flaw in the IMDS at the CSP level enabled data leakage through SSRF attacks

In July 2019, an external entity gained access to the databases of a major American bank and succeeded in leaking the personal details of some 100 million American citizens, and of 6 million Canadian citizens.[21]

The attack included several stages: in the first stage, the attacker detected an existing vulnerability in the CSCs web server with a reverse proxy capability. In the second stage, the attacker exploited the abovementioned vulnerability to execute an SSRF attack. In the third stage, the SSRF attack enabled the attacker to gain access to IMDS version v1.0. In the fourth stage, due to flawed design, IMDS v1.0 enabled the attacker to run metadata queries about the resource (despite the fact that the attacker came from the Internet), and in this way to gain access to the credentials at the resource's disposal. Finally, the attacker exploited the credentials that it obtained in the previous stage to access the CSCs S3 bucket, and to copy the data to another S3 bucket in its possession.[22][23]

[20] CloudImposer: Executing Code on Millions of Google Servers with a Single Malicious Package
https://www.tenable.com/blog/cloudimposer-executing-code-on-millions-of-google-servers-with-a-single-malicious-package
[21] Information on the Capital One cyber incident
https://www.capitalone.com/digital/facts2019
[22] Cloud Instance Metadata Services (IMDS)
https://www.sans.org/blog/cloud-instance-metadata-services-imds-/
[23] How an Attacker Could Use Instance Metadata to Breach Your App in AWS
https://www.skyhighsecurity.com/threat-research/how-an-attacker-could-use-instance-metadata-to-breach-aws.html

Inadequate isolation between the CSP customers' environment enabled an attacker to leap from one to the other

In this incident, an attacker that gained a hold in the environment of one customer, managed to leap \ initiate lateral movement to the environment of another customer due to inadequate isolation, such as the absence of suitable segmentation and segregation between different customers, or use of the same instance of IAM system to manage different customers, thereby widening the scope (blast radius) of the ransomware attack. Including leakage of sensitive information. Note that several such incidents were seen primarily in small to medium CSPs.

Flawed implementation of a SAML token enabled impersonation

The SaaS platform gave CSCs SSO based access via a SAML token. Due to flawed implementation, existing CSCs could change the content of the SAML token, and thereby impersonate a user associated with a different CSC.[24]

Taking over of a CSP system administrator's account gave the attacker access to customers' resources

An attacker that managed to take over a CSP system administrator's account providing identity, authentication and access control management services, harvested authentication details (such as access tokens) from the system, enabling it to access the customers' resources.[25]That is, by using a supply chain attack, the attacker managed to gain access to the customers' resources.

Attacks on CSCs

[24] Microsoft Office365 SAML Vulnerability: Authentication Bypass https://www.ssocircle.com/en/2361/microsoft-office365-saml-vulnerability-authentication-bypass/
[25] Understanding the Okta supply chain attack of 2023: A comprehensive analysis https://blogs.manageengine.com/it-security/2024/01/25/understanding-the-okta-supply-chain-attack-of-2023-a-comprehensive-analysis.html

A Golden SAML attack enabled access to sensitive information

Golden SAML is the term applied to an attack that enables an attacker to expand its hold on-premises organizational infrastructure and to access the existing resources in the CSCs public cloud environment.

Similar to a Golden Ticket attack against on-premises organizational infrastructure, this assault enables the attacker to impersonate a CSCs legitimate user, giving it access to the CSPs existing resources.[26][27] The attack can be executed by using several methods, such as stealing the private key of the ADFS installed in the CSCs on-premises organizational infrastructure, and signing a forged SAML token. In the last stage, the forged SAML token was used to gain access to resources stored in a public cloud environment.

Through the use of this attack, several attackers were able to obtain sensitive information from various organizations stored within a public cloud environment, including data housed on widely recognized SaaS platforms. This occurred despite the fact that, initially, the attacker did not possess the access credentials for the environment in question.[28]

A ransomware breakout after the transfer of assets to an alternative server room

In 2023, two companies migrated assets to an alternative server room, and because the assets contained ransomware that no one was aware of, ransomware breakout occurred, which spread throughout the network, resulting in the encryption and loss of data of the company itself and of its customers. Including deletion of backups. [29][30]

[26] Golden SAML Attack
https://www.netwrix.com/golden_saml_attack.html
[27] Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps
https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps
[28] UNC3944 targets SaaS applications
https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications
[29] CloudNordic loses most customer data after ransomware attack
https://www.techtarget.com/searchsecurity/news/366549773/CloudNordic-loses-most-customer-data-after-ransomware-attack
[30] Danish cloud host says customers 'lost all data' after ransomware attack
https://techcrunch.com/2023/08/23/cloudnordic-azero-cloud-host-ransomware/

Multistage attack that led to a permanent shut down of a company's business operations

In 2014, a company experienced a multi-stage attack. In the first stage, the attacker launched a DDoS attack. The attack was likely designed to distract the company's attention from the next stages of the attack. In the second stage, the attacker managed to gain access to the company's AWS Management Console, and demanded a ransom as a condition for stopping the DDoS attack. The company changed its credentials for the AWS Management Console, but the attacker had created alternative accounts in advance that enabled it to maintain its hold for a long period of time. After the attacker realized that the company was not planning to pay the ransom, it began deleting data and resources from the AWS environment, including EBSs and content stored in S3 buckets. As a result, the data of both company and customers were lost, including backups, ultimately leading to a permanent shutdown of the company's business operations.[31]

Storage of secrets in a cloud service for GitHub source code management

The GitGuardian 2024 report found that over 12.8 million new secrets were exposed in 2023 (such as API keys, access tokens, encryption keys, passwords and usernames) that had been stored on GitHub public repositories (public cloud service for managing Github source code). Certain secrets facilitated subsequent (cascading) attacks, including gaining unauthorized access to the CSCs public cloud environment and causing data leakage.[32] Upon infiltrating the CSCs public cloud, attackers often exploit this access to conduct coordinated assaults, including phishing campaigns and targeted supply chain attacks, with the objective of disseminating ransomware.[33]

Quite often, what generates these cyber incidents is the absence of effective secure development, such as the lack of adherence to accepted recommendations for cloud

[31] Code Spaces Destroyed by Cyber Attack
https://www.esecurityplanet.com/networks/code-spaces-destroyed-by-cyber-attack/
[32] The State of Secrets Sprawl 2024, GitGuardian
https://www.gitguardian.com/state-of-secrets-sprawl-report-2024
[33] AndroxGh0st – the python malware exploiting your AWS keys
https://www.lacework.com/blog/androxghost-the-python-malware-exploiting-your-aws-keys

development, including guidance on the use of designated means to secure secrets, such as KMS or HSM. As well as the absence of periodic scanning to detect secrets in source code and flawed access control.

Leakage of access keys enabled the attacker to leak information and to extort the CSC

An attacker that succeeded in gaining hold of access keys to a CSCs public cloud environment executed a multistage attack. In the first stage, the attacker used access keys to gain access to data in an S3 bucket. In the second stage, the attacker leaked the information from the S3 bucket. In the third stage, the attacker neutralized the version control mechanism. In the fourth stage, the attacker deleted the contents of the S3 bucket. In the final step, the attacker confirmed that the S3 bucket did not include any previous versions and left a ransom note demanding payment.[34]

Exposure to Ransom DDoS (RDDoS) attacks

It is commonplace for cyber attackers to exploit the CSCs vulnerability to Ransom DDoS (RDDoS), and CSCs that don't agree to the terms of the ransom or don't have a suitably robust system of security suffer lasting financial and other losses. Thus, for example, execution of an RDDoS attack lasting several hours or more may incur the CSC high charges from the CSP. Furthermore, this exacerbates the consequences associated with the compromised availability of business services.

Application of weak access control enabled penetration of a SaaS email platform

Many organizations that used a SaaS email platform did not apply suitable access control. For example: did not enforce use of multifactor authentication (MFA). As a result, the attacker managed to obtain the login password, and via it, to access cloud services and cloud data. In certain instances, the attacker configured rules that directed a concealed copy of both outgoing and incoming messages from the user's

[34] Ransomware in the cloud
https://www.invictus-ir.com/news/ransomware-in-the-cloud

mailbox to another mailbox under their control. In this way, the attacker maintained a hold even after the user changed the login password.

Common attack vectors in public cloud environments

Common attack vectors in public cloud environments. Note that the CSC must undertake periodic risk assessment and map the attack vectors relevant to its risk profile.

Misconfiguration exploits

The public cloud offers high accessibility to services and data from anywhere, from any device, at any time. Gaps in the professional skills of those who engage in the field is commonplace, due in part to heavy workloads and to task diversity, rapid changes in the business environment and the requirements of the various stakeholders, the broad range of service offerings available in a public cloud, the wide assortment of CPSs in the market, and the adoption of advanced concepts, such as DevOps, which transfer some of the control to parties for whom information security and cybersecurity are not their core function. At the same time, many organizations don't have an effective change management process in place, and also don't use established controls to minimize the realization of risks.

Cloud misconfigurations can expose the services and data to all Internet users. Including exposure to malicious acts by hackers. According to information published, this is a very common attack vector.

Flawed design of multi-tenant architecture

Use of a public cloud is based on sharing of resources between CSCs, known as a multi-tenant architecture. However, cloud providers, especially the smaller ones, often don't isolate CSCs adequately from one another. This increases the likelihood of lateral cyber incidents. Thus, for example, one CSC may receive access to the data of another CSC. Another example is a cyber incident in which one CSC can "leap" to the environment of another CSC. As a last example, an attacker may exploit a vulnerability in a shared access component, enabling use of one CSCs credentials to access the data of another CSC.

Use of open source code that contains a backdoor or other vulnerability

Open source code is widely used today, but many CSCs are not sufficiently aware that the code may contain malicious implants, such as a backdoor, or malware designed to take advantage of the existing computing resources in order to mine digital coins (cryptomining), etc.

As a result, the development team and/or the ICT team may use open source code (such as tools, code libraries, copying of sample code available in commonly used data repositories) that contains vulnerabilities, backdoor etc., thereby granting attackers partial or full access to the environment.

For more details, see: OWASP Top 10 Risks for Open Source Software[35]

Lack of adequate protection for secrets

The use of secrets is highly prevalent at the infrastructure and application levels, including source code for cloud automation processes. The secrets that the CSC may also use include API Keys, User/Passwords, Digital Certificates, etc.

Organizations frequently fail to implement adequate safeguards for their secrets, resulting in the storage of such data in plaintext within source code or various storage locations in the cloud environment. Frequently, also without applying appropriate access control, and also without using the mechanisms recommended by the CSPs, such as KMS or HSM.

In addition, there is a trend towards using source code management (SCM) in a public cloud environment, which may include sharing information with the public and/or with third parties, such as in the form of outsourcing, and even sharing of source code developed by a CSC as part of open source projects.

All these increase the likelihood of secrets being exposed to unauthorized entities. And this in turn, is liable to enable extensive access to the existing resources in the public cloud environment.

[35] OWASP Top 10 Risks for Open Source Software
https://owasp.org/www-project-open-source-software-top-10/

For details, see: OWASP Top 10 CI/CD Security Risks[36]

API interfaces are vulnerable without suitable security

Direct exposure of API interfaces with a vulnerability and/or without the application of acceptable security mechanisms, such as API GW/ WAAP, make it easier for an attacker to gain access to sensitive data.

For details on the subject, see: OWASP Top 10 API Security Risks[37].

Shared vulnerability in public cloud services

According to the shared responsibility model (SRM), the CSP bears responsibility for lateral issues, such as infrastructure security. In the event that a shared vulnerability is exposed, for example, the CSCs are usually dependent on the CSP to apply the necessary fix. In many cases, the CSCs are not aware of the existence of the vulnerabilities in the provider's services at all. Applying the fix depends on several parameters, such as the provider's ability to fix what needs to be fixed, and the service level agreement (SLA) defined and enforced between the parties. In some cases, after the fix is applied, the customer may be required to perform follow-on actions, such as a reboot of virtual machines.

Note that vulnerabilities published by CPSs together with critical updates (Day-1) may make execution of malicious acts possible, including ransomware attacks. An example of this is the vulnerability in a CSP service published in September 2022 that effectively enabled privilege escalation by an external entity[38].

Sometimes, new vulnerabilities are published (Zero-Day) that enable misuse of public cloud services, such as initiation of an attack from the cloud environment against the CSC or against a third party. An up-to-date example of this is the exploitation of a

[36] OWASP Top 10 CI/CD Security Risks
https://owasp.org/www-project-top-10-ci-cd-security-risks/
[37] OWASP Top 10 API Security Risks
https://owasp.org/www-project-api-security/
[38] https://securitylabs.datadoghq.com/articles/appsync-vulnerability-disclosure/

critical vulnerability in the OneDrive service, which enabled attackers to encrypt the data and delete backups, while bypassing accepted security measures[39].

Exploitation of file syncing mechanisms, replication and transfer of information to an archive

Cloud services include syncing of files between an end point and the cloud, replication at the region level, the option of applying replication between regions, and transferring data to an archive. Some of these mechanisms are usually enabled by default, sometimes without the CSCs awareness. Users often run these services from an end point while bypassing regular ICT processes (Shadow AI / IT), in order to reduce response times and overcome organizational barriers that compromise productivity and/or innovation.

The attacker may inject a malicious file with the aid of a file syncing mechanism that searches for new files or new versions of files for uploading to the cloud. Mostly, the malicious file will arrive via a phishing or spear phishing email as an attachment to a message that attempts to emulate a harmless file or a link that allows downloading the file (A Drive-by Download Attack). Once the file is downloaded, the service automatically uploads the file to the cloud platform, where it spreads to shared folders in the cloud; and when the files are accessed more malicious actions can be perpetrated.

In cases where ransomware encrypts the files at a particular end point for example, the attacker may execute file syncing and/or replication and/or transfer of information to an archive in order to update or overwrite backups stored in a public cloud, with the aim of harming or even preventing the CSCs ability to recover should the need arise.

[39] https://i.blackhat.com/BH-US-23/Presentations/US-23-Yair-One-Drive-Double-Agent-Clouded-OneDrive-Turns-Sides.pdf

Breached credentials

There are several possible ways of obtaining credentials for a cloud platform with the aid of credentials obtained maliciously. The following are several common techniques:

1. With the aid of Info-Stealer run on the CSCs end-user computers (including web browsers), which steals passwords and monitors keystrokes, collecting authentication details directly when users access cloud services.
2. Leakage of credentials auctioned on the Darknet, phishing campaigns of varying degrees of complexity, or purchasing of credentials leaked in a previous incident (credential stuffing), or other methods.
3. Brute-Force attacks, and the like, in order to run through an exhaustive series of default or weak passwords or all the options for a password.
4. Scanning of code repositories and public professional forums in order to find secrets.

A cyber attack based on predictable resource names

A cyber attack exploiting predictable resource names occurs when an attacker can easily guess the names of resources, such as S3 buckets, within an environment. This vulnerability can lead to unauthorized access if appropriate security measures, like access policies, are not implemented. The use of predictable names heightens the risk of exploitation, potentially resulting in data breach or account takeover etc..[40]

Social Engineering

There are several social engineering techniques that target users on a cloud platform. The following are several common techniques:

1. Phishing/ spear phishing scams that seek to obtain a username and password by employing landing zones that display a "fake" login to cloud services.

[40] AWS CDK Risk: Exploiting a Missing S3 Bucket Allowed Account Takeover, Aqua Security, October, 2024 https://www.aquasec.com/blog/aws-cdk-risk-exploiting-a-missing-s3-bucket-allowed-account-takeover/

2. Adversary-in-the-Middle (AitM) attacks [41]to obtain information that may help attackers gain access to cloud platforms. In such cases, the attack presents a login page to cloud services, and if the login also incorporates a multifactor authentication (MFA) component, the attacker can obtain it using steps similar to regular phishing scams, but using more complex capabilities. In June 2023, Microsoft identified such an attack that sought to gain access to their services[42][43].
3. A vishing (phone call phishing) scam in which the attackers impersonate a legitimate party, mostly IT personnel, and obtain the details or persuade the victim to connect to a phishing page.
4. A mobile text messages (SMS) phishing scam (Smishing), in which the attacker impersonates a legitimate party, usually by sending a message in the name of the CSP or the CSC about the need to change a password or confirm identifying details or update the means of payment, and harvests information and/or persuades the user to connect to a phishing page.

There are also attack vectors that specifically target SaaS environments:

Exploitation of an existing vulnerability in the Federations infrastructure

The Federation infrastructure (such as ADFS) enables organizations to deploy SSO, which eliminates the need to manage multiple identities for a single user, and improves the user experience.

The following are several ways attackers often assault a Federation infrastructure:

1. An attacker that gains access to the Federation infrastructure may be able to issue forged credentials (such as an SAML token), thereby granting the attacker access to resources in the public cloud.

[41]This attack is sometimes also called an Evilginx attack, based on the name of an open-source tool that attackers often use in cyberspace

[42] New Mamba 2FA bypass service targets Microsoft 365 accounts https://www.bleepingcomputer.com/news/security/new-mamba-2fa-bypass-service-targets-microsoft-365-accounts/

[43] Detecting and mitigating a multi-stage AiTM phishing and BEC campaign https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

2. Exploitation of an existing SaaS vulnerability allows an attacker to replace the legitimate URL that is meant to direct the user to the legitimate IdP with a malicious URL that redirects the user to a different website where the user's credentials are harvested. This attack is also known as SAMLjacking.

Transfer of information by the CSP to sub-providers without the CSCs knowledge and consent

CSPs with SaaS platforms often use a number of sub-providers, such as a secondary CSP that provides OCR services or to "Whitening"/"Data Sanitization". Very often, the CSC is not aware that its sensitive information is being passed to another CSP that is under no real obligation to the CSC. In addition, a CSC often does not have a real ability to guarantee the secondary CSPs level of security, and that it complies with the requirements of the law and the regulations etc.. In view of this, a cyber incident at a secondary CSP may result in exposure of the CSCs sensitive information to unauthorized entities, and an attacker may even leap from the secondary CSP environment to the primary CSP environment.

Setting up of a new user account before access by a legitimate user

The attacker first sets up a new user account on a SaaS platform with an identical name to a legitimate user account that already exists at the CSC. The attacker then defines secondary recovery channels (such as an email address or telephone number) in the account that it set up.

Next, the legitimate user tries to register for the service and receives a message that the account already exists. The user usually tries to recover the password (for example, by clicking the Forgot Your Password link), resets it, and proceeds to work as usual. At some point or another, the attacker resets the password using an alternative channel, thereby regaining a hold on the account. This attack is also called Account Ambushing.

A web vulnerability that enables penetration of the cloud environment and/or exploitation of the identification interface

An attacker may exploit a web vulnerability that enables penetration of the cloud environment and/or exploitation of the identification interface.

The following are several common techniques adopted by attackers:

1. Exploitation of a known web vulnerability, such as one of those appearing in the OWASP Web Security Testing Guide.[44]
2. Misconfiguration of the session management mechanism, so that the access token of a disabled account is valid, granting access to services and data. This is a frequent issue in independent configuring of protocols such as OAuth 2.0 and OpenID Connect.
3. Absence of a validation mechanism (such as validation of a digital signature or other mechanism) to check that the access token has not been subjected to involuntary modification and is not impersonating a legitimate one.
4. Use of a protocol for a purpose for which it was not intended, such as use of OAuth 2.0 to authenticate a user even though the purpose of the protocol is only to allocate authorizations.

Use of CSCs' legitimate cloud environments as an infrastructure to attack third parties (watering hole attack/ Living off the Land - LOTL)

In recent years, many attackers have expanded their capabilities and techniques to sneak into the public cloud using trusted websites and legitimate services in order to evade detection and identification, while concealing the existence of command and control (C2) communication as seemingly normal, legitimate traffic or as harmless messages being transferred on online platforms (LOTL).

As a result, attackers often use CSCs' legitimate cloud environments as a launchpad to attack third parties.

Below are several examples:

[44] OWASP Web Security Testing Guide
https://owasp.org/www-project-web-security-testing-guide/

1. In data leakage from an entity, the attacker may transfer the organizational information to an object database in a public cloud under its control. Data leakage is a typical tactic used in ransomware attacks.
2. Setting up of a command-and-control server in a public cloud environment that communicates with the ransomware run in the entity's environment.

This technique often allows cyber attackers to bypass regular security mechanisms, such as geolocation. The security measures and/or the end-users put greater trust in sites stored in public cloud environments, especially when the object names presented to the users (such as part of the URL) use characteristics they identify as being safe (such as the name of the organization or of the CSP).

Social Engineering in a SaaS environment

Over the years, attackers have developed several techniques with characteristics unique to SaaS users. Below is a review of several commonly used techniques:

1. Sending phishing messages by email or via an instant messaging service or via QR code that includes a URL at which the user is called upon to grant the attacker permissions via the OAuth 2.0 protocol. Users that receive a message multiple times tend, in many cases, to ultimately approve the request to grant access permissions, enabling the attacker to gain a long-term hold. Note that even after the user session has ended, and even after the user has changed the password, the attacker's hold is retained until it is manually removed.
2. Publishing of an imposter app in the official or in an imposter marketplace or on a website, and then employing phishing or vishing to persuade the user to download and install the malicious application. A similar technique is used by attackers to disseminate a malicious plug-in.
3. Using homoglyph characters to bypass security measures such as spam filters, and to deceive users.

Naturally, the above list of attack vectors is not exhaustive. Each CSC should therefore create a registry of the attack vectors relevant to it, based on its own risk profile.

To build a bank of attack vectors, use generally accepted sources of information as an aid, such as:

- Top Threats Working Group, Cloud Security Alliance (CSA) publications
- ENISA publications, such as Threat Landscape
- Publications by OWASP, such as: Cloud-Native Application Security Top 10, and OWASP Testing Guide
- MITRE publications, such as MITRE ATT&CK® Cloud Matrix, and MITRE ATLAS
- SaaS Attack Techniques
- Reports and publications regarding Living Off the Cloud (LOTC)
- Reports and publications by public cloud providers
- Reports and publications by information security and cybersecurity companies, such as companies that specialize in cyber threat intelligence (CTI)

Recommended Courses of Action for Mitigating the Risk of Cyberattacks in Public Cloud Environments

This section presents recommended courses of action for mitigating the risk of cyberattacks in public cloud environments, categorized in accordance with the NIST Cybersecurity Framework (CSF) 2.0[45].

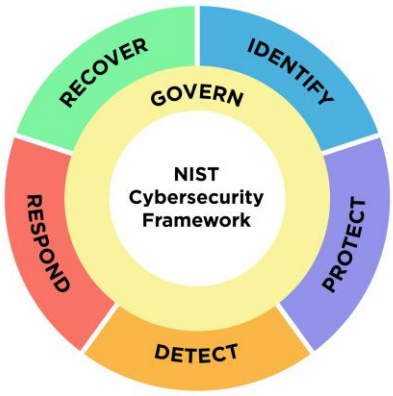


Figure 4: The Cybersecurity Framework (CSF) 2.0 Categories

Note that the recommended courses of action for mitigating risk reviewed in this document are not exhaustive and focus on the ransomware threat. The organization must conduct a periodic risk assessment, and adjust the courses of action it uses to mitigate risk to the requirements of the Law and the regulations, the contractual requirements and the business needs.

The accepted approach to information security and cybersecurity today adopts the principles of Threat-Informed-Defense and Evidence-Based Defense.[46]

[45] NIST Cybersecurity Framework (CSF) 2.0, NIST, February 26, 2024
https://www.nist.gov/cyberframework
[46] Cybersecurity: Center for Threat-Informed Defense
https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/

The governance category: GOVERN

Consolidating and supervising the organization's policy and strategy on cyber risk management. [47]

Risk management strategy (GV.RM)

The organization should develop a risk management strategy that includes the cloud, and clearly define its priorities, constraints, level of risk acceptable to the organization, starting assumptions in the decision making on these issues, and clear-cut principles for when and how the risks are to be treated (accept, reject, transfer, mitigate). The strategy must also include mapping of and reference to all the requirements, as expressed by the stakeholders at the CSC and outside it, including customers (consumers) and providers.

The risk management strategy must also address situations in which a nesting cloud is used by the CSC itself or by another CSP that serves as a secondary provider. The strategy should include periodic examination of the exit plan or termination of the contractual engagement with the CSPs, including defining of clear and up-to-date criteria about when to invoke it.

The strategy should include periodic examination of the need to purchase cyber insurance, while it should also be verified that the policy includes reference to work in a public cloud environment. In addition, the strategy should ensure that the data protection officer (DPO) be included in information security and cybersecurity activities, and serve as a permanent member on the relevant steering committees.

The chief information security officer (CISO) should appoint a specially designated person to manage cloud governance, risk, and compliance (GRC).

For more details, see: SaaS Governance Best Practices for Cloud Customers[48]

[47] The meaning of the category names are taken from the "Defense Maturity of Small and Medium Businesses Questionnaire" published by the Israel National Cyber Directorate in 2024.
[48] SaaS Governance Best Practices for Cloud Customers, CSA, October 10, 2022

CSPs' Cloud Adoption Framework (CAF) documentation

Policy (GV.PO)

The information security and cybersecurity policy should include reference to the unique challenges and risks in working in a public cloud environment, and the application of accepted indicators (such as KCI, KGI, KPI, KRI, OKR) to examine the implementation process as well as the effectiveness of the risk management strategy.

Supply chain security (GV.SC)

The CSC should establish definitive criteria for selecting the CSP, including a preliminary and periodic analysis as to how effective the native tools are against the latest attack vectors, based on the organizational risk profile.

Below are several examples of criteria:

1. As a prerequisite for the CSPs contractual engagement, it must comply with CSA STAR[49] Level 2 or FedRAMP Moderate (Level 2)[50] certification requirements or higher, and the scope of the certification must cover the resources relevant to the CSCs activities.
2. The CSP exhibits economic resilience and compliance with open and accepted principles of corporate governance.
3. The CSP enables the CSC to maintain data sovereignty.
4. The CSP enables data portability between different CSPs using accepted technology (such as API), and supports open standards/ formats. This issue is essential for backups and business continuity.
5. The CSP offers the CSC consultations with the information security and cybersecurity team, which also responds to regular issues.
6. The CSP offers CSCs an eDiscovery service, which helps investigations. The CSC must also verify that accepted compliance requirements are met.

https://cloudsecurityalliance.org/artifacts/saas-governance-best-practices-for-cloud-customers

[49] CSA STAR
https://cloudsecurityalliance.org/star

[50] FedRAMP
https://www.fedramp.gov/

7. The CSP offers support for open standards that aid efficient and effective management, and that reduce the likelihood of misconfigurations and errors in the implementation of the security policy. For example: SCIM.
8. The CSP has a Digital Forensics and Incidents Response (DFIR) team and 24/7 cyber monitoring services.

Recognition of a shared responsibility model

The shared responsibility model (SRM) is a cornerstone of the cloud security concept, because it draws a clear distinction between the CSPs commitment on information, cyber and privacy defense issues and the CSCs commitment on those issues.

Note that despite the name "shared responsibility model", many legal and regulatory requirements view the CSC as having sole responsibility for information security, cybersecurity and privacy protection issues. Therefore, switching to the services of this or that CSP does not replace or absolve the CSC of sole responsibility for these issues.

Before entering into a contractual engagement with a CSP, it is vital that the CSC check the shared responsibility model between the parties, and examine whether it is compatible with the risk profile and the risk level acceptable to the organization. If, during the contractual engagement, changes are made to this model, CSC management must periodically examine the implications of this. Equally important is the timely assessment of the effective and efficient enforcement of the contract.

IDENTIFY category

Identifying the present status of the cyber risk to the organization.

Asset management (ID.AM)

The CSC should define a continuous process for discovery and mapping assets (such as data, hardware, software, systems, facilities, services, providers, personnel, data centers, zones, regions, APIs), and analyze their interdependencies. The CSC should

also possess technological and other means to build data flow diagrams on the basis of the actual situation and history, and in relation to the real-time mapping and history of the business/ operational processes (process flow diagram).

Given that there is no one set of terminology used by all the CSPs, it is vital that a unified table be built to map assets. The following is a common example: the terminology for a segregated environment may vary between different Cloud Service Providers (CSPs). For instance, Azure refers to it as a Virtual Network (VNet), whereas Google Cloud Platform (GCP) and Amazon Web Services (AWS) use the term Virtual Private Cloud (VPC), and Oracle Cloud Infrastructure (OCI) employs the term Virtual Cloud Network (VCN).

Its recommended to enable the VPC logs (they are not usually enabled by default), and use made of complementary capabilities, such as CSPM and DSPM. This will ensure that the mapping of the relevant assets is available to the decision-makers and to the information security and cybersecurity team. An approach that can assist, among other objectives, in identifying Shadow AI / IT activities.

In the next stage, it is important to define each asset's sensitivity level/ criticality (Durability[51]) according to the business impact analysis (BIA), which will help to improve the effectiveness and efficiency of the security practices, such as a risk assessment, business continuity plan (BCP) and disaster recovery plan (DRP).

Consideration should be given to the fact that the CSP may offer several configurations for assigning assets to an IAM [52]in the public cloud, where each configuration has its own strengths and weaknesses.

The following is a short review of common configurations for the assignment of assets to IAM in the public cloud.

[51] Durability - Durability refers to the expected average annual data loss, typically quantified as a probability of loss over a given period (for example, a year).

[52]The term IAM is used in the public cloud of AWS and OCI. While the Azure public cloud uses the term Entra ID, and GCP uses the term Cloud Identity

- **Registered Devices configuration** may be suited to BYOD assets, but offers the CSC a "low" degree of command and control.
- **Joined Devices configuration** is suited to CSC owned assets, and grants a "high" degree of command and control.
- **Hybrid Joined Devices configuration** is suited to a situation in which an organization is in the stages of transferring its assets to a public cloud. This configuration generally grants a "high" degree of command and control.

It is therefore important that the CSC define which parties are authorized to assign assets to IAM and in what manner, and define periodic controls to verify that there are no dormant (inactive) or malicious assets.

Risk assessment (ID.RA)

It is good practice to ensure that the risk assessment addresses the following issues:

1. Inclusion of the organizational assets and the supply chain.
2. Attack vectors and TTPs of ransomware and of leading attack tools.
3. Periodic vulnerability scanning, both in the CSC environment and at the level of the CSP.
4. Use of cyber threat intelligence (CTI) to improve resilience and the risk assessment process.
5. Performance of a periodic Privacy Impact Assessment (PIA) as outlined by the Privacy Protection Authority.[53]
6. Deriving lessons learned and insights from local and global cyber incidents.

[53]The Authority publishes a methodological guide to conducting a Privacy Impact Assessment - a tool to help organizations assess and mitigate privacy risks, the Privacy Protection Authority, November 23, 2022 https://www.gov.il/he/pages/taskir_privacy_news

Striving for continuous improvement (ID.IM)

The CSCs should conduct periodic exercises to examine the competency and readiness to cope with a cyber incident, and carry out measurements to learn lessons and strive for continuous improvement.

For more details, see: Cyber exercises - building and conducting the organization's cyber exercises[54]

PROTECT category

Application of protections to prevent or mitigate the cyber risk.

Identity management, authentication, and access control (PR.AA)

Multifactor Authentication (MFA)

Use of additional factor in the authentication process during login to the public cloud environment adds a crucial and valuable layer of defense. An authentication mechanism comprising only username and password has serious security limitations, providing attackers with a simpler penetration path. Adding another authentication factor via a special app that supports a real-time challenge/ response mechanism makes it difficult for a malicious outsider to log in. In the case of administrator accounts with elevated privileges or users with a sensitive role (such as users with extensive access to PII), use of FIDO II compliant hardware authentication devices should be considered as they are more resilient in the face of attacks, such as an AiTM attack.

Experience has shown that requiring successful MFA to complete a sensitive operation (such as disabling file versioning in an S3 Bucket) constitutes an effective and low-cost security measure.

[54]Cyber exercises - building and conducting the organization's cyber exercises, the Israel National Cyber Directorate, December 2022
https://www.gov.il/he/pages/cyberexercise

Note that use of a fixed login password and a temporary password received via an SMS or email message does not constitute MFA, but rather 2SV - Two Step Verification.
In the light of this, it should be verified that MFA is enforced for all the users. For example: use of a fixed password combined with biometric authentication or with a smartcard containing a private key.

Use of conditional access policies

Conditional access policies enable a CSC to implement granular access control, also known as risk-based authentication and continuous authentications.
In this framework, user and asset (such as an endpoint) compliance with accepted parameters is checked before the authentication process and throughout the session, even if the user was originally successfully authenticated.
Below are several common parameters:

1. User and Location (Context)
2. Application
3. Real-Time Risk (Threat Intelligence, ML Risk Score etc.)
4. Device, including checking the state of the cyber hygiene
5. Target resource (virtual machine, data, etc.)

Conditional access policies often enable enforcement of the following rules:

1. Allow Access
2. Block Access
3. Required MFA
4. Limited Access
5. Password Reset
6. Monitor Access

The use of conditional access policies offers a balance between operational and security needs. This increases the likelihood that a user logging in to the cloud environment is an authorized user and originates from a "healthy" environment.

Access control and access policy in a public cloud

In many attacks, the attacker gains a hold by exploiting misconfiguration of access permissions to the existing resources in a public cloud.

CSPs frequently allow the application of permissions on two levels:
- Access control applied to users and entities via an IAM system.
- An access policy applied to resources (such as an S3 bucket) often allowing bypassing of access control restrictions.

In the light of this, it is vital to be thoroughly acquainted with the CSPs work methods, and its approach in the event of a conflict between access control definitions and the access policy. It is also important to apply the principles of Least Privilege, Need to Know, Need to See and Separations of Duties (SoD), while organizations with a complex environment are advised to seek a CIEM solution or equivalent. This will reduce the likelihood of human error that would lead to a cyber incident and/or violation. Organizations should also utilize a CSPM solution for real-time monitoring of the security posture and to detect gaps, such as needless exposure of resources to the Internet.

Consideration must be given to the fact that a Cross-Deployments Role (such as a Cross Account when working with AWS) can often be applied in a public cloud, which expands the scale of access to user accounts. This sometimes enables access from the CSC environment of one body to the CSC environment of another body.

Secrets security

Secrets are widely used in a cloud environment, and disclosure of a secret to an unauthorized party can easily end in a significant cyber incident.
In the light of this, CSCs are advised to adopt the following steps:

1. Define and enforce work procedures that prohibit users from storing secrets in unauthorized configurations.
2. Define systematic work practices for managing the lifecycle of secrets. Including a focus on periodic changes and minimizing of human intervention.
3. Adopt mechanisms for storing secrets that are in accordance with the CSPs recommendations, subject to their compliance with the requirements of accepted standards, such as FIPS 140-3 Level 2, or higher. For example: KMS or HSM.
4. Use cloud native scanning tools and other tools for continuous detection of the existence of secrets in the various resources, including in the source code.
5. Apply secrets detection practices in the CI/CD pipeline (such as performing a validation during the code commit process), and prevent continuation of the build process until what needs fixing is fixed.

Use a mechanism that grants ephemeral (temporary) access (Just-in Time Admin)

CSPs often allow high-privileged accounts (such as network administrators that access the CSPs management console) ephemeral access to assets (Just-in Time Admin), which reduces the time window available to an attacker to perpetrate malicious acts, such as identity theft. Some CSPs also enable application of other security mechanisms, such as applying a requirement for receipt of approvals/ confirmations from two independent approvers (dual control) before access is granted to the production environment. Use of these mechanisms makes it much more difficult to execute an attack that has a lateral impact. Such as the dissemination of ransomware or deletion of existing assets at the CSP.

Define break glass accounts

Define break glass accounts to be used should the need arise. In order to secure such accounts, MFA must be implemented along with other restrictions, such as granting of access from specific IP addresses only. These accounts must be monitored continuously in case an attacker manages to gain a hold on them.

Awareness and training (PR.AT)

While cloud IT processes are, to some extent, similar to those in on-premises organizational infrastructure, there are also many differences in the work methods, platform offerings and accessible tools that facilitate agile, distributed work spanning territorial borders; but at the same time, operation and security personnel don't always fully comprehend the implications of the differences.

In view of this, it is vital to promote awareness and training for personnel involved in IT practices, in order improve risk management and application of the necessary controls, alongside mitigation of the likelihood of a significant cyber incident occurring due to human error (misconfiguration).

Useful, free sources of information include publications by the Israel National Cyber Directorate, the Cloud Security Alliance (CSA[55]), the American National Institute of Standards and Technology (NIST)[56], the Center for Internet Security (CIS)[57] and leading cloud providers.

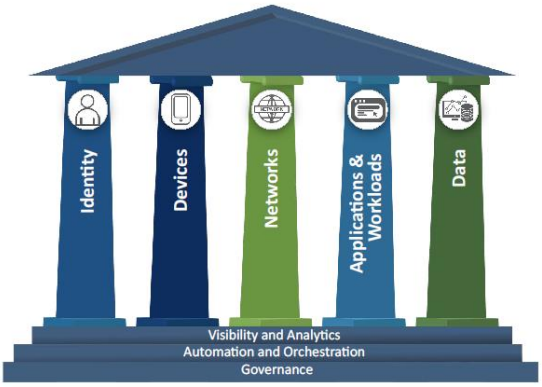
Technology infrastructure resilience (PR.IR)

Implementation of a Zero-Trust Maturity Model

The latest concept of security, also known as the zero-trust model, is based on the principle of "never trust, always verify". That is, there is no computer or entity that can be blindly trusted, and therefore, continuous verification is required.

The American CISA organization developed a four-level model of maturity that enables organizations to gradually adopt the principle, including application of it to the five pillars.

[55] https://cloudsecurityalliance.org/
[56] https://www.nist.gov/cybersecurity
[57] https://www.cisecurity.org/

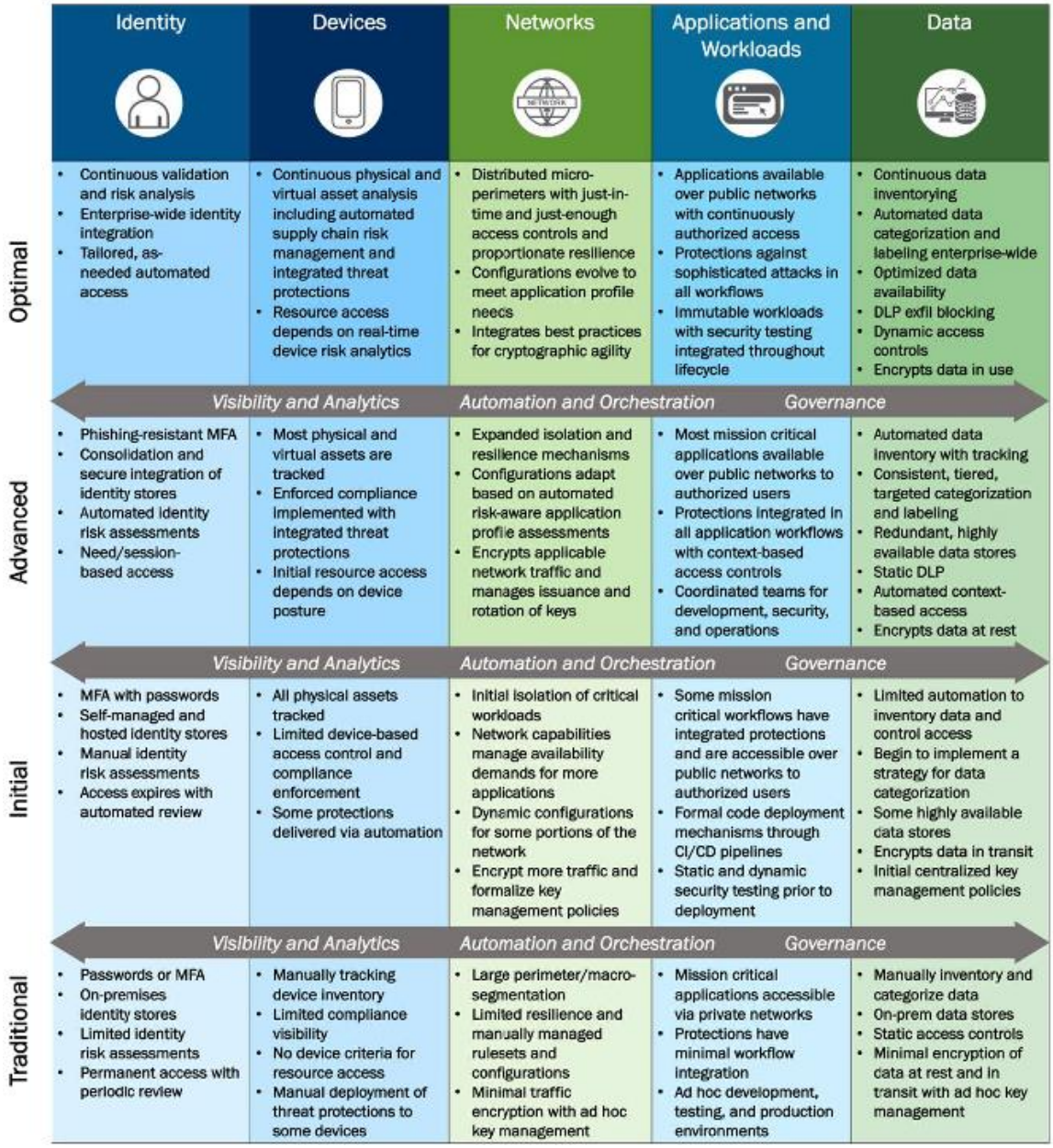


[58]

Figure 5: The Pillars of the "Zero Trust Model", according to the CISA model of maturity

The following table presents the model of maturity's four levels. The transition from one level to the next increases the degree of visibility and situational awareness about the level of exposure, while providing clear-cut recommendations about which controls need to be applied in order to strengthen the resilience.

[58] Zero Trust Maturity Model, CISA, April, 2023
https://www.cisa.gov/zero-trust-maturity-model



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile neecs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

[59]

Table 5: Maturity levels according to CISA's Zero Trust Model

Given the brevity of this paper, a full review of the maturity model is not feasible; however, several key highlights for adoption by CSCs are presented.

[59] Zero Trust Maturity Model, CISA, April, 2023
https://www.cisa.gov/zero-trust-maturity-model

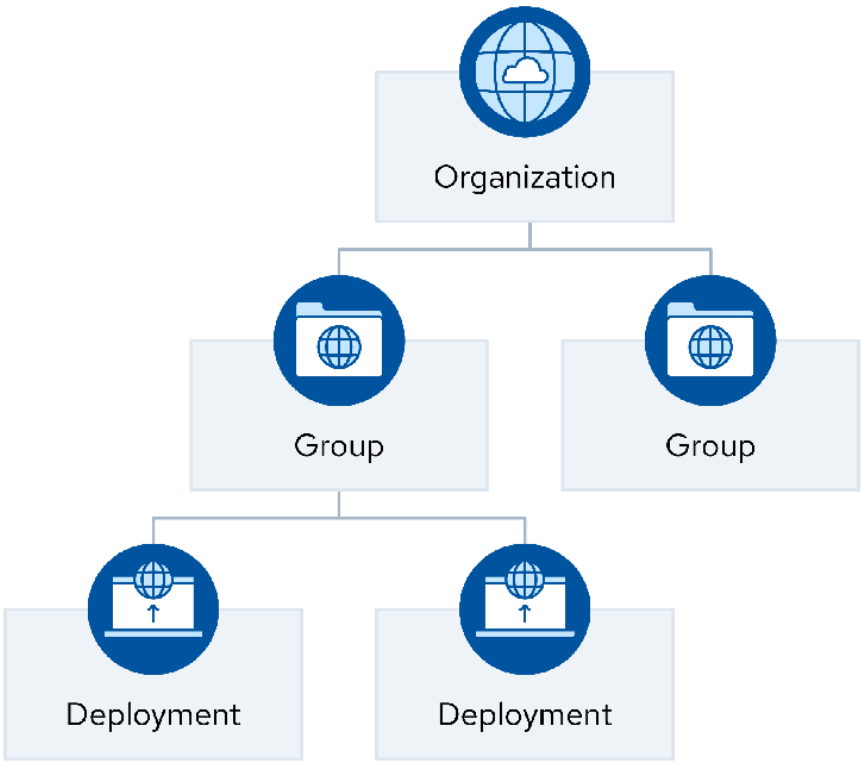
Proper planning of a typical hierarchy of resources in a public cloud environment

CSPs often allow construction of a hierarchy of resources to enable separation of environments, granular segmentation/ segregation, and mitigation of the blast zone if a cyber incident or other adverse event occur.

The typical model contains a "parent organization", under which "groups" are defined, each of which can contain one or more environments for "deployment". Environments that share the same group may have a shared policy applied through inheritance (as a mandatory requirement or as an option that is subject to change) from the parent organization level or at the level of the group itself.

It is also good practice to apply a policy at the deployment environment level that is aligned with the top-level policy that was outlined.

The following diagram presents a typical hierarchy of resources in a public cloud environment:



[60]

[60] Security Guidance for Critical Areas of Focus in Cloud Computing v5, CSA, July 15, 2024

Figure 6: A typical hierarchy of resources in a public cloud environment

Given that the terminology differs from one CSPs to another, the terminology employed by the major CSPs is presented in the table below:

Deployment	Group	Organization	Cloud Service Provider
Accounts	Organization Unit	Organization	AWS
Sub-Compartment	Root-Compartment	Tenancy	Oracle Cloud Infrastructure (OCI)
Projects	Folders	Organizations	GCP
Subscriptions	Resource Group	Tenant	Microsoft Azure

61

Table 6: The terminology employed by the major CSPs

Below are several key recommendations for proper planning of the hierarchy of resources in a public cloud, including defining of the landing zone:

1. It is recommended to use the Well-Architected Framework as an aid to proper planning of the organizational hierarchy, including factoring in of the operational and security challenges. Some of the CSPs provide the CSCs with tools (such as Account Factory) to implement the recommended hierarchy and build a landing zone, while minimizing the need to manually set up the hierarchy of resources (both during the initial setup, and during recovery in an emergency). These tools

https://cloudsecurityalliance.org/artifacts/security-guidance-v5

[61] The table was built based on the concept in the document entitled: Security Guidance for Critical Areas of Focus in Cloud Computing v5, CSA, July 15, 2024
https://cloudsecurityalliance.org/artifacts/security-guidance-v5

often employ Infrastructure as Code (IaC), and may therefore help recovery from a disaster.

2. It is recommended to verify that the protocols and services used do not contain any known vulnerability (such as IMDS v1.0), and that it is impossible to set up new resources that use protocols and services with a known vulnerability. Additionally, some CSPs offer the option to enhance security at the IMDS level by implementing measures such as restricting traffic based on the VPC ID and/or the IPv4 address of the virtual machine.[62]
3. It is recommended to implement a policy that defines in advance where, at the physical and logical level, new resources can be set up, and to where roaming of existing resources can be undertaken. This simplifies realization of accepted principles for effective and efficient data governance.
4. Implement a policy designed to minimize the risk of accidental or malicious resource deletion. For example, in AWS, configure the "Unlock Delay Period" or enable "Rule Lock" to enhance resource protection.
5. It is recommended to ensure that when creating new resources, their attributes (such as S3 Bucket Naming) are random, so the likelihood of an attacker being able to predict them is minimal. It is also recommended that information, such as AWS Account ID, which can be used to predict resource attributes (such as S3 Bucket Naming), be classified as sensitive data. Access to this information should be restricted to authorized individuals only to prevent misuse and protect the integrity of the resources.
6. It is recommended to ensure that once resources are no longer in use, their old links are removed from the list of resources. For example, the link to an S3 Bucket that previously stored JavaScript directories and was deleted should be removed from the website's code.
7. Design the organizational security policy (such as SCPs - Service Control Policies and RCPs - Resource Control Policies in AWS and RBAC) and inheritance processes

[62] How to use policies to restrict where EC2 instance credentials can be used from https://aws.amazon.com/blogs/security/how-to-use-policies-to-restrict-where-ec2-instance-credentials-can-be-used-from/

in a manner that minimizes human error that could cause exposure. The preference is for PoC (Policy as Code).

Role-Based Access Control (RBAC) is a model for granting permissions based on the type of role that a user or resource (such as a virtual machine) plays, where it is important to apply the following security principles: Least Privilege, Need to Know, Need to See, SoD.

It is worth noting that the actual implementation method of this model may differ from one CSP to another.

For example, in AWS, a virtual machine can be assigned a role that grants access to resources such as an S3 Bucket, by defining an IAM Instance Profile:

Resource Control Policies (RCPs) allow you to centrally and consistently restrict access permissions to resources. For example: You can restrict access to S3 Buckets in a blanket manner by defining which user accounts and from which Deployments can access them.

Service Control Policies (SCPs) allow you to centrally and consistently restrict the permissions that can be assigned to user accounts, such as defining which IAM Roles can be assigned to a particular user account.

8. Plan the operational policy, such as the tag names policy and the permissible location for setting up of new resources, in a manner that helps minimize human error, which could lead to exposure and/or other violation.
9. Verify that the security logs are transferred to a specially designated deployment environment that will be assigned a high level of segmentation/ segregation.
10. It is rare in routine times for the CSCs ICT team to execute operations at the organization level and/or to use entities at this level (such as high-privileged

accounts). Therefore, make sure that the cyber monitoring covers this issue. Separations of Duties (SoD) must be applied, such that one management entity cannot make changes at this level.

11. During VPC to VPC connectivity (and the like), use technology that transfers the data on the CSPs back plane, to verify that the data is not passed onto the Internet. For example: AWS PrivateLink.
12. When creating a new resource or transferring an existing resource to another deployment, verify that accepted security requirements are automatically applied to it, such as the security patches deployment policy, activation of logs that are not normally enabled and a copy sent to a data lake and/or to the SIEM system, as well as deployment of a CWPP agent.
13. Implement a policy that prevents deletion or modifying of sensitive resources (Resource Lock).

The document also addresses the "maintenance of backups and information security", detailing proper design of a typical hierarchy of resources in a public cloud environment.

Architecture design for a SaaS platform operated by a CSP

Organizations that seek to use a CSP SaaS platform are not always sufficiently aware of important issues liable to create significant security gaps. Thus, for example: the issue of isolating customers from each other that share the same resources on a SaaS platform is often an Achilles' heel. Another example is that organizations seeking to build a SaaS platform at a CSP are not aware that the CSPs offer different technologies, such as VPC endpoints and a dedicated communications line between the customer site and the CSP network (such as AWS Direct Connect), which greatly reduce the attack surface. Use the CSPs' guides as an aid; they include explanations and instructions on how to set up and manage a SaaS platform.

In designing the architecture for a SaaS platform, make sure that reference is made to the use of WAAP/ WAF/ RASP as a corrective control. The CSC should use an SSPM solution as a corrective control, and not rely exclusively on the CSPs security system.

For more details, see: Design SaaS on AWS[63]

Deployment of malware countermeasures

Malware countermeasures should be deployed, such as CWPP at all the in/out data gateways and also in the resources themselves. Consider the following issues:

1. The CWPP solution maker is often the CSP itself, and a nesting cloud is sometimes used when third-party security solutions are deployed.
2. Verify that the CWPP solution transfers logs to the monitoring system as soon as possible, given the short lifespan of resources (e.g. a container) in a public cloud environment.
3. The CSC should possess a security solution in the event of roaming of assets between different environments, such as on-premises, a public cloud environment and work from home.
4. Verify that the solution chosen is capable of providing an optimal security response to work in a BYOD configuration. For example: implementation of accepted security capabilities in an EMM/ MDM solution.
5. Verify that the solution chosen is capable of using digital forensics to extract artifacts from the various resources in order to enable execution of an effective investigation.
6. When receiving files at in/out gateways, accepted CDR ("Whitening"/"Data Sanitization") checks should be incorporated. It is important to perform repeated

[63] Design SaaS on AWS
https://aws.amazon.com/saas/design/

checks (I.e. Retro-Hunting) on files that were previously defined as safe, as they may later be discovered that they are part of a known attack campaign.

7. Verify that the solution chosen is capable of providing an effective response against Zero-Day and 1-Day threats.
8. Verify that the solution chosen presents the findings according to the latest version of the MITRE ATT@CK Framework, and that the maker maintains optimal coverage in respect of its latest versions.
9. It is recommended to ensure that up to date version of the selected solution is employed, to guarantee access to the latest capabilities and to mitigate the risk of known vulnerabilities.
10. It is important to ensure that the chosen solution includes an FIM module that is properly implemented and active.

Deploy countermeasures to contend with DDoS attacks

Deploy countermeasures against DDoS attacks. Make use of the CSPs native tools and/or those of third parties. Address the following issues:

1. Verify that the solution chosen provides an optimal response to different types of DDoS attacks (such as volumetric attacks, protocol attacks, and application layer attacks).
2. It is recommended to ensure that the selected solution is configured in an 'Always-On' mode.
3. Verify that the solution chosen provides a continuous monitoring mechanism to detect DDoS attacks and that acts to enable the CSC to continue its normal business operations, while taking operational steps to neutralize the attacker's infrastructures.
4. CSPs generally offer several levels of security against DDoS attacks. The CSC should adopt a level of security that includes continuous monitoring and granular handling of adverse events by the CSP, such as taking down of the attacker's infrastructures.
5. Use of CDN and autoscaling of IT resources are effective and efficient in mitigating the impact of DDoS attacks. These capabilities should therefore be adopted during

the design and implementation of the architecture, with periodic fine-tuning undertaken according to threat landscape updates.

6. It is recommended to ensure that the selected solution is capable of decrypting traffic, identifying threats, and neutralizing them. To safeguard the private key, it is advisable to employ a KMS or HSM solution that complies with the FIPS 140-3 Level 2 standard or higher.
7. It is recommended to utilize the principles of Chaos Engineering to continuously assess the resilience of the environment.

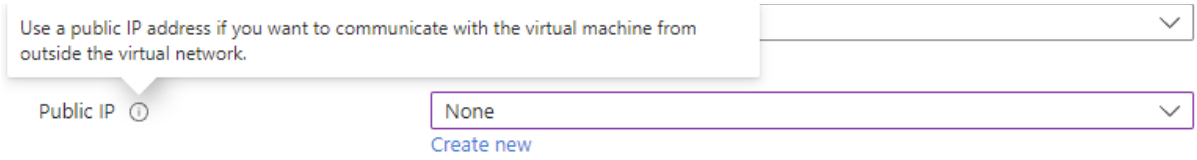
Network segmentation and segregation

Implementing network segmentation and segregation principles makes it difficult for attackers to execute lateral movement in order to gain a sweeping hold on assets. Below are several key recommendations for implementing segmentation and segregation:

1. Define the rule set such that all traffic is denied by default. Note that some of the CSPs adopt a policy permitting outbound and/or other permissive traffic by default; the default settings for the ruleset should therefore be changed during the provisioning of the environment and of the various resources.
2. Proper restriction of the connectivity between the building blocks of the network and the various resources enables isolation, making it difficult for the attacker to gain a hold. Therefore, proper design of the VNet/ VPC as well as of the network access control list (NACL) and the network service groups (NSGs) is vital, including periodic examination of the existing security posture in relation to the risk profile. The recommendation of leading CSPs is to deploy micro-segmentation so that each asset functions in its own dedicated network environment, accessible on the basis of Least Privilege Access.
3. When implementing load balancing (LB), it is advisable to ensure that all incoming traffic from the Internet is routed through the LB. Additionally, it is crucial to avoid the presence of any network interface card with a public IP address that is directly exposed to the external network.

Verify that the CSP allocates a dedicated VXLAN/ Geneve ID to each VPC (or equivalent). Utilizing a VLAN for network segmentation and segregation is no longer regarded as an effective approach.

4. Relatively large organizations and/or those with a complex environment and/or sensitive data should use a dedicated next-generation firewall (NGFW) that is set up in the network transit hub, so that the access control policy can be centrally enforced, and greater visibility achieved.
5. In the case of resources that don't need direct access to the Internet, allocate IP addresses that cannot be routed to the outside world.
   Below is an example for applying the above definition ("None") when a new virtual machine is created in Azure:



6. It is recommended to enable VPC Flow Logs and monitor for anomalies.
7. Consider recording the traffic to there in order to improve the visibility. This can be usually be achieved by enabling port mirroring at the resource level (such as a virtual machine), and mirroring the traffic to a sensor.

Change management and the application of configuration settings

Change management and configuration settings are a cornerstone of IT processes, and their proper application should help the CSC mitigate the likelihood of human error that could lead to a cyber incident.

It is therefore recommended that the CSC examine implementation of the following:

1. **Examine the security posture of the environment on a continuous basis in relation to an accepted baseline -** by continuously examining the environment

in relation to an accepted baseline, such as the latest CIS Benchmark, security gaps can be detected, such as permissive firewall rules.

2. **Use native tools to save the approved configuration settings** - cloud native tools, such as AWS Config can be used to detect unauthorized changes/ configuration drift, and to restore the desired state automatically or semi-automatically.
3. **Use IaC** - the use of IaC can help ensure that the environment maintains its desired state and, if necessary, facilitate disaster recovery by provisioning a new environment and transferring the data to it.
4. **Password management policy** - the password management policy should prevent the possibility of using default passwords, and also prevent the possibility of using previously leaked passwords. Apply a policy mandating the use of long and unique passwords and verify that each password does not exist in regular password repositories (such as repositories of passwords that have been leaked in the past, default passwords, passwords known to be weak, rainbow tables). Also verify that changing of passwords is an automated process by using PIM / PAM or other solution.
5. **Enforce secrets security mechanisms** - using accepted security mechanisms, such as KMS, for secrets security increases the likelihood that they will not be overtly accessible to attackers. Verify that the secure development process requires that all versions of the software (including versions in the development and testing stages) employ these mechanisms by default. As a corrective control, the source code and assets should be subjected to periodic testing in order to detect storage of secrets in violation of the organizational policy.
6. **Prevent access to management interfaces** - access to the management interfaces (such as RDP and SSH) of assets such as virtual machines and containers should be blocked by default. As an alternative to logging in to a virtual machine, a bastion host that reside in a private network or AWS SSM or other secure solution can be used.

Serverless architecture security

Serverless architecture offers advanced operational capabilities, generally available to all CSCs by default. To minimize the possibility of exploitation of a serverless architecture, adoption of the following is recommended:

1. Log the lifecycle of the functions' activity.
2. Assign the principle of Least Privilege and ensure that it is consistently applied, even in scenarios involving function chaining (e.g., when one function invokes another).
3. Verify that a serialization attack cannot be perpetrated against a function.
4. Command-and-control of the software components built into the functions. Including the use of SBOM for documenting the contents.
5. Verify that the functions' software components are included in the organizational vulnerability scanning and handling process.

For more details, see: How to Design a Secure Serverless Architecture[64]
OWASP Serverless Top 10[65]

Secure Development

A CSC that develops software and/or purchases software from a third party and/or adopts open source code should verify that the software meets accepted requirements for secure development, such as:

- Secure by Design and Secure By Default
- Privacy by Design and Privacy By Default

It is also recommended that the CSC adopt proactive approaches in which information security and cybersecurity requirements are integrated both during the early stages

[64] How to Design a Secure Serverless Architecture, CSA, October 23, 2023
https://cloudsecurityalliance.org/artifacts/how-to-design-a-secure-serverless-architecture
[65] OWASP Serverless Top 10
https://owasp.org/www-project-serverless-top-10/

of development (Shift Left) and after the product is released and deployed in the production environment (Right Shift).

The CSC should adopt the CSPs secure development recommendations and verify that the service or product meets accepted requirements, such as the OWASP Application Security Verification Standard (ASVS), security verification Level 3[66] and OWASP MASVS (Mobile Application Security Verification Standard) security verification Level 3[67].

The CSC should have an up-to-date copy of the software bill of materials (SBOM) for the software components that it uses. CSCs that use a SaaS platform should have the contract specify that the CSP provide them with a SaaSBOM for every version. The CSC can then integrate the SaaSBOM/ SBOM in its vulnerability management process, which contributes to an informed risk management process.

For more details, see: SSDF NIST SP 800-218[68]

CISA SBOM[69]

CISA Open Source Security[70]

OWASP Top 10 Proactive Controls[71]

[66] OWASP Application Security Verification Standard (ASVS)
https://owasp.org/www-project-application-security-verification-standard/
[67] OWASP MASVS (Mobile Application Security Verification Standard)
https://mas.owasp.org/MASVS/
[68] NIST SP 800-218
Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST, February, 2022
https://csrc.nist.gov/pubs/sp/800/218/final
[69] CISA SBOM
https://www.cisa.gov/sbom
[70] CISA Open Source Security
https://www.cisa.gov/opensource
[71] OWASP Top 10 Proactive Controls
https://top10proactive.owasp.org/

Securing artificial intelligence (AI) capabilities

Use of a public cloud grants CSCs convenient access to advanced artificial intelligence capabilities, be it an off-the-shelf GenAI service, or a GenAI service as a basis for a chatbot that delivers a customer service solution, or access to infrastructure and tools in order to adapt existing models to various business needs or to develop new models from scratch. etc. The CSC should therefore verify that it has deployed and activated security measures throughout the lifecycle in order to protect the artificial intelligence capabilities that it uses. The CSC should have an up-to-date copy of the AIBOM for the artificial intelligence components that it uses. The CSC can then integrate the AIBOM in its vulnerability management process, which contributes to an informed risk management process.

For more details, see: Principles, Policy, Regulations and Ethics in the Area of Artificial Intelligence 2023[72]

NIST AI RMF[73]

NIST AI RMF Playbook[74]

ISO/IEC 42001:2023 AIMS[75]

MITRE ATLAS [76]

AI Model Risk Management Framework[77]

[72]Principles, Policy, Regulations and Ethics in the Area of Artificial Intelligence 2023, the Ministry of Innovation, Science and Technology, December 14, 2023
https://www.gov.il/he/pages/ai_23
[73] NIST AI RMF v1.0, NIST, January 2023
https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development
[74] NIST AI RMF Playbook, NIST, March 30, 2023
https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook
[75] ISO/IEC 42001:2023
Information technology — Artificial intelligence — Management system
https://www.iso.org/standard/81230.html
[76] MITRE ATLAS
https://atlas.mitre.org/
[77] AI Model Risk Management Framework, CSA, July 23, 2024
https://cloudsecurityalliance.org/artifacts/ai-model-risk-management-framework

Command-and-control of registration and use of applications, plug-ins, and the marketplace

The CSC should take acceptable measures to maintain command-and-control of the registration and use of applications, plug-ins, and the marketplace. A Deny by Default policy should be adopted, and registration and use of applications, plug-ins, and marketplace permitted on a granular basis. It is also good practice to verify that the permissions allocated to the development team to register new applications (including alpha and beta versions, etc.) do not allow them distribute an application and plug-in to the production environment and/or to legitimate users without receipt of advance approval, according to the CSCs approved change management procedure.

Consideration should be given to the fact that many SaaS platforms allow users to access the marketplace by default, enabling them to download new applications, new plug-ins and/or to add new functionality. In certain cases, the organizational data may be transferred to a third party, such as a secondary CSP. In the light of this, prior to using a SaaS platform, the CSC should establish a clearly defined information security and cybersecurity policy outlining systematic practices for approving the use of applications/plug-ins and adding of new functionality.

Platform security (PR.PS)

Reducing the attack surface and implementing hardening

It is advisable to take periodic action to reduce the attack surface and to implement hardening. Also, give consideration to the following issues:

1. Reduce the number of management interfaces accessible from the Internet, both at the level of the CSP management interfaces, and at the level of the various platforms. As an alternative, a bastion host and other solutions can be used.
2. Install security patches periodically, as frequently as befits the risk profile. Install security patches on assets with direct exposure to the Internet within 24 hours of their publication.

3. Use aids such as the CIS Benchmark to detect security gaps in the CSC environment, and to close them as soon as possible.
4. Harden the platforms in accordance with acceptable methodologies, such as CIS (level 2 at least) and [78]DISA STIG[79] (level 2 at least).
5. Remove and disable software components and services that are not required in normal business operations. Including filesharing services.
6. Verify that the platform security covers the relevant TTPs, and implements the relevant security mechanisms in accordance with the D3FEND Matrix[80].

Securing virtual machines and containers

Generally speaking, the cloud concept is that any resource (such as a virtual machine and a container), apart from the data itself, is ephemeral (transient). Another prevalent concept is that changes are not made to an asset/ infrastructure in the production environment (immutable). Changes that need to be applied are executed by deploying a new asset, and removing the old one. Adoption of these concepts enables the CSC to reduce the attack surface, and to achieve faster recovery in the case of a cyber incident or operational fault.

In addition, apply hardening practices is vital. For example: neutralization of management interfaces and preventing the ability to log in locally. All these narrow the attacker's window of opportunity, an important step in strengthening organizational resilience.

Organizations can use CWPP and other security solutions as a corrective control.

Another issue is command-and-control over the process for choosing the images to be deployed, in order to ensure that the images don't contain malicious code. The CSC should therefore work with a trustworthy image/ container registry; and, as part

[78] CIS Benchmarks
https://www.cisecurity.org/cis-benchmarks
[79]DISA STIG
https://public.cyber.mil/stigs/
[80] D3FEND Matrix
https://d3fend.mitre.org/

of the CI/CD process, the trustworthiness of the software components is tested by tools such as ASPM.

Service Mesh Security

Service Mesh Security approach refers to the set of practices, policies, and tools used to ensure the confidentiality, integrity, and availability of communication between microservices in a distributed application architecture. A service mesh typically manages the interactions between microservices by providing security functionality like traffic management, load balancing, and service discovery. Securing these interactions is essential to prevent potential security threats such as unauthorized access, data breaches, or service disruptions.

Key aspects of service mesh security include:

1. **Authentication and Authorization:** Ensuring that only authenticated and authorized services can communicate with each other. This is often achieved using mutual TLS (mTLS), which encrypts traffic and authenticates both the client and server.
2. **Encryption:** Encrypting traffic both in transit and at rest to protect sensitive data. Service meshes often provide automatic encryption for inter-service communication.
3. **Traffic Management:** Implementing secure routing and policies to control the flow of traffic between services (e.g. east-west traffic), preventing unauthorized or malicious traffic from entering the system.
4. **Identity and Access Management (IAM):** Assigning and enforcing fine-grained access policies based on the identities of services, ensuring that each service only has access to the resources it needs.
5. **Audit and Monitoring:** Continuously monitoring service-to-service communication and logging interactions for audit purposes, enabling the detection of unusual or suspicious activities.

6. **Policy Enforcement:** Enforcing security policies at the service mesh level, such as rate-limiting, retries, and circuit breaking, to mitigate potential attacks like DoS or DDoS. Additionally, some solutions enable the implementation of policies that restrict access to outdated versions of services.

Securing API interfaces

To secure API interfaces, adoption of the following points is recommended:

1. **Reduced exposure** - preventing direct exposure of the CSCs APIs to the world, by using an API GW that enforces a security policy. Including:
   - **a.** Enforcement of schema and content validation according to a list of predefined parameters (allowlist).
   - **b.** Enforcement of a strong authentication method consistent with the risk profile. Below are several examples:
     1) An API designed for M2M will use mTLS.
     2) An API designed for H2M will use MFA.
   - **c.** Enforcement of a token management method consistent with the risk profile. Below are several examples:
     1) Digital signing of a token or use of another security technique.
     2) Use of a token that does not create a security gap. For example: as a rule, a JWT token can be used in operations in the CSCs internal environment, but not for users located outside this environment (for example: an end customer who logs in to the site from their endpoint at home).
   - **d.** Limiting the number of requests in a particular time window that a specific API is capable of responding to (API throttling).
   - **e.** Limiting the number of requests that a single client can make to a specific API in a particular time window (rate limiting).
   - **f.** Limiting access to an API according to geolocation.
   - **g.** Application of an access permissions management model consistent with that required, such as fine-grained.

h. Logging of requests and transferring them to an information security and cybersecurity team for analysis.

i. Implement version control and refrain from using outdated APIs.

2. **Secrets security** - use of the means recommended by the cloud provider to store secrets.
3. **Secure development** - verifying that the API interfaces were developed in accordance with acceptable principles for secure development, and that each version is tested using accepted automated tools (such as ASPM / DAST / IAST / SAST / SCA), a code review and resilience testing. Securing the token and session management process is also very important. Use can also be made of accepted standards such as OpenAPI [81]in order to validate the application in practice.

Verifying that the SCA supports scanning of open source code libraries that are stored with clear text, as well as libraries that are stored as binary code, such as compiled code.

Use of SASE

Organizations that use a number of cloud services and/or have a large number of branches should investigate the possibility of using a SASE solution as an alternative to the traditional VPN solution. Use of a SASE solution enables centrally controlled application of the security policy, high visibility, plus an enhanced customer experience (UX), which may be expressed in the provision of a response to requests from the server farms near their geographic location, guaranteeing quick response times. Another no less important reason for preferring SASE is that significant security gaps have been discovered in traditional VPN solutions in recent years, that take a very long time to fix. And on many occasions, the fix published has not been effective and/or has created a significant business vulnerability. In addition, the fix was often

[81] OpenAPI
https://www.openapis.org/

found not to repair the underlying problem because secure methods were not adopted in the development of the VPN solution, such as Secure by Design and Secure by Default. This is led to recurrent security problems arising from the same underlying problem.

Securing a SaaS message (such as email) sending platform

It is accepted practice for the CSP to provide the infrastructure for messaging (such as email) in a SaaS configuration. The platform usually enables two work configurations:

1. Application-to-Application (A2A)
2. Application-to-Person (A2P)

To minimize the possibility of exploiting a SaaS messaging platform, adoption of the following is recommended:

1. Periodically verify that the list of recipients meets the CSCs business needs.
2. Periodically verify that the Pub/ Sub settings, including the applications/ services that can interact, meet the CSCs business needs.
3. Apply security measures during sending/ receiving, such as a DMARC mechanism and defining of a BIMI record, as well spam and malware filters.
4. Apply a clear definition of acceptable message types and attributes (such as size, frequency of sending).
5. Conduct periodic sampling to verify that the contents of the messages do not include anomalous data.

Secure on-premises

Take action to secure on-premises organizational infrastructure, including the management endpoints and the identity management system (such as AD). Furthermore, to improve visibility, deploy a CASB solution at the points of access to public networks, such as the Internet. This can also help contend with threats from Shadow AI / IT operations.

When deploying Federation infrastructure, make sure that the servers exposed to the Internet have WAF/ WAAP protection.

The following are examples of common AD attacks against which the CSC should ensure a suitable level of resilience:

No.	Attack Name
1.	AD Enumeration
2.	AdminCount
3.	adminSDHolder
4.	ASREPRoast \ Authentication Server Response (AS-REP) Roasting
5.	BloodHound Reconnaissance
6.	DCShadow
7.	DCSync
8.	Default/Hard-coded Credentials
9.	Diamond Ticket
10.	ESC15 (Escalation paths in AD CS)
11.	Forge IPv6 Gateway
12.	Golden Ticket
13.	Kerberoasting
14.	LDAP Anonymous Login (Binding)
15.	LDAP Injection
16.	Local Loop Multicast Name Resolution (LLMNR) Poisoning
17.	MachineAccountQuota Compromise

No.	Attack Name
18.	Misuse Access Control List (ACL) Misconfiguration
19.	NBT-NS Poisoning
20.	NTDS.dit Extraction
21.	NTLM Relay
22.	Pass-the-Hash (PtH)
23.	Pass-the-Ticket (PtT)
24.	Password Spraying
25.	PetitPotam NTLM Relay Attack on an Active Directory Certificate Services (AD CS)
26.	SAML Golden Attack
27.	SID History Injection Attack
28.	Silver Ticket
29.	Skeleton Key Attack
30.	Unconstrained delegation
31.	Wdigest: Extracting Passwords in Cleartext
32.	WPAD

Table 7: Examples of common AD attacks against which the CSC should ensure that adequate resilience exists

Note that the above list is not an exhaustive list of the attacks against which the CSC should verify that adequate resilience exists.

The following are good practices to adopt during CASB deployment:

1. Verify that deployment architecture is inline deployment.
2. Verify that encrypted traffic is opened before it reaches the user in order to detect and thwart threats in the encrypted medium.
3. Verify that the chosen solution is capable of detecting common P2P applications, and implement a security policy accordingly that is aligned with the CSCs requirements. Including provision of a response to applications that use WinSocket and Reverse Tunnel and Web 3.0 (such as applications that use the IPFS protocol).
4. Verify that the chosen solution has a UEBA capability.
5. Verify that the chosen solution has a DLP capability.
6. Verify that the chosen solution has an RBI capability.

Data security (PR.DS)

Encryption of data in the cloud

Encryption is efficient in mitigating the effectiveness of cyber incidents, and ransomware in particular. in the light of this, it is good practice to verify that data stored in the cloud are encrypted by default throughout their lifecycle. By incorporating security principles such as SoD, the encryption key can be defined as not normally having access to the user account, so that even if an attacker manages to steal an identity in order to exfiltrate data from the CSC environment, it will have little ability to decrypt the data.

Cloud encryption can be implemented at several levels, as shown in the figure below; the CSC should therefore examine an encryption method in relation to its risk profile.

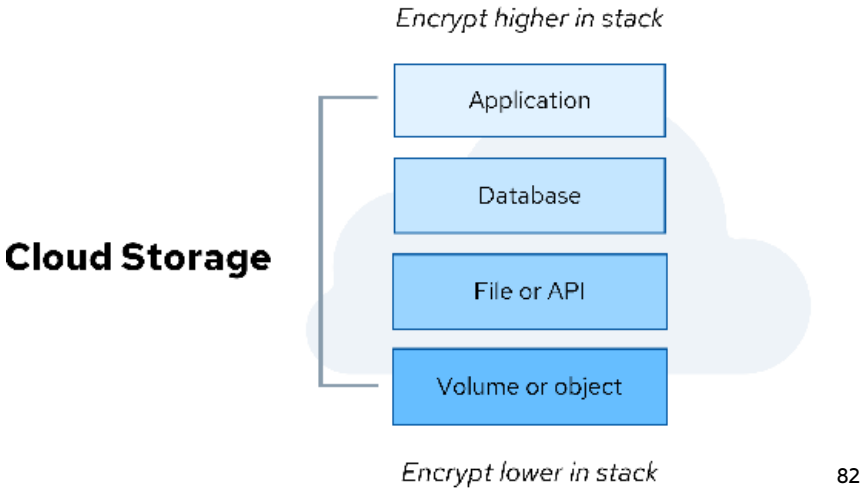


Figure 7: The layers that encryption can be applied to for data security purposes

[83]Confidential Computing

"Confidential computing" is a cloud computing technology that protects data during processing of it \ at runtime. The technology's operating principle is based on allocation of a Trusted Execution Environment at the CPU level; only those software components approved by the CSC are allowed access to the processing and its deliverables.

It is good practice to use this technology as a corrective control when working with sensitive data repositories.

Data leak Prevention (DLP)

Given the fact that attackers often leak organizational data to Internet servers before the data is encrypted and a ransom demanded, deployment of data leak prevention countermeasures may diminish the attacker's ability to achieve its goals. At the very

[82] Security Guidance for Critical Areas of Focus in Cloud Computing v5, CSA, July 15, 2024 https://cloudsecurityalliance.org/artifacts/security-guidance-v5

[83] Also sometimes called "secret computing"

least, they may be an important source of telemetry to help the CSC detect an attack in the making, before the attacker starts to encrypt the data.

In addition, applying systematic data governance at the CSC level can greatly assist detection of the data's location, classification of it, improve the data leak prevention countermeasures, and serve as proof that the CSC meets the compliance requirements. Many legal and regulatory requirements place the onus on the CSC to manage this type of process for reasons other than just information security and cybersecurity, such as protection of privacy, and protection of intellectual property and safety.

The DLP solution should ensure compatibility with various configurations in the public cloud, such as the use of storage based on object database, queues, databases utilizing diverse technologies (e.g. NoSQL, vector database), and media streaming services.

Privacy-Enhancing Technologies

Privacy-Enhancing Technologies (PET) include a wide variety of hardware and software solutions designed to maximize the value of the personal information (commercial, scientific, and social) managed by an organization, while mitigating the risk to the privacy of the data subject and keeping this data secure.[84] One of the most well-known solutions is the masking of sensitive data, such as credit card details.

Deployment of PET in the CSC environment is an effective and efficient way of mitigating the impact of the damage in a ransomware attack. In contrast to on-premises organizational infrastructure where the organization has to execute full deployment and maintenance of a solution over time, a significant number of CSPs offer managed solutions that can be deployed at relatively short notice, without high overheads.

[84] Table Top Number 31: Privacy Enhancing Startups - Trends and Challenges https://govextra.gov.il/media/o15lb2gr/table-31.pdf

Realization of the Data Minimization principle

Periodically examining the data status and taking proactive steps to minimize excess assets (such as data, obsolete virtual machines) are effective and efficient in mitigating the impact from the outbreak of a ransomware attack in the CSC environment. Moreover, realization of this principle has several inherent advantages, such as compliance with the requirements of the relevant laws and regulations, and lower cloud service consumption costs.

Maintenance of backups and data security

In some cases, foreign entities may be involved in holding the data in an cyber incident, deletion or encryption of data, most of which occur during ransomware attacks, but also in other attacks. Storing and maintaining backups is a key step in recovery from such an incident. Important points and good practices for maintaining backups and for data security:

1. **User quota -** limit set on the amount of resources (such as storage, processing power, or network bandwidth) a user can consume within a system or VPC. This ensures fair usage, prevents abuse, and maintains system performance. For example, in cloud services, user quotas might limit the number of files a user can upload or the amount of storage they can use. In addition, it also helps in efficiently managing resources and preventing system overloads and excessive financial consumption of resources.
2. **Periodic validation -** is essential when working with backups. The backup must include a full restore of the assets to a dedicated environment (sandbox), followed by operational validation, such as simulation of user access to the environment and feeding in/ extracting of data.
3. **Detecting malware in backups -** by periodic scanning of data supported by up-to-date signatures (retro hunting), and by using more advanced investigation capabilities, such as running in a dedicated testing environment (sandbox).
4. **Detecting anomalies in backups -** detecting anomaly in backups including correlation with the backup history, such as an exceptional backup volume,

changes in file entropy levels compared to previous levels, and obscure changes in file extensions.

5. **Protected storage of backups** - ransomware attacks often attempt to delete, corrupt or encrypt backups. Therefore, use the CSPs native DR services and archive services to store backups, such that they are normally read only [similar to the traditional Write Once Read Many (WORM)]. In addition, access control should be defined such that only specific authorized individuals have access to backups. If possible, define that access to backups require the advance approval of independent approvers.

Minimize the possibility of running software/ tools in the backup storage environment, in order to prevent the ability to execute ransomware stored in backups. Such execution may stem from human error, an over-enthusiastic ICT staff seeking to perform a quick restore, or malicious intent.

6. **Allocation of a dedicated hierarchy of resources for saving backups** - allocate a specially designated and independent hierarchy of resources for saving backups, so that even if an attacker manages to take over control of the production resources hierarchy and/or the DRP resources hierarchy and/or system administrator endpoints, the attacker's ability to compromise the integrity of the backups would be extremely low. Also use dedicated hardware for the system administrator endpoints, and independent means of authentication (such as a specially designated FIDO II hardware card), etc.

The following is a diagram of a recommended typical resources hierarchy:

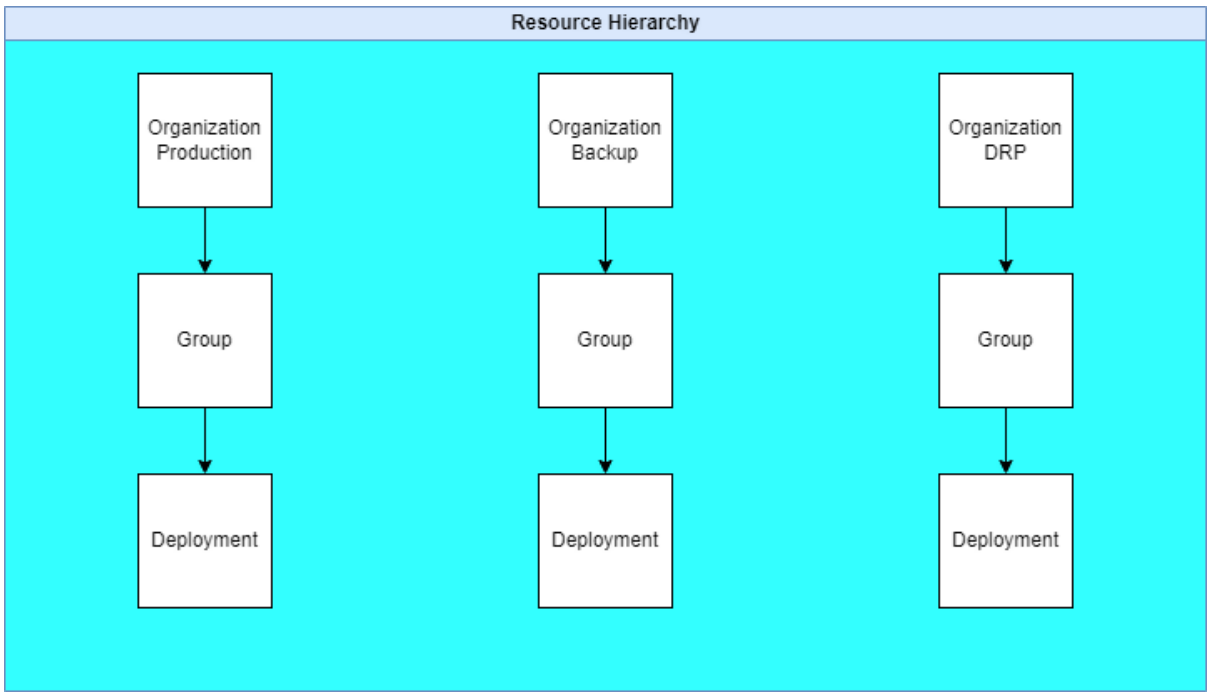


Figure 8: A recommended typical resources hierarchy

Generally speaking, it is good practice to allocate a specially designated and independent non-DRP hierarchy for backup storage. The main aims of the recommendation are:

- To verify that the backups won't be damaged even if assets are transferred with active ransomware from the production environment to the DRP environment.
- To verify that the backups won't be damaged in the event that backup data are restored and run.

In the event of concerns about an insider threat, consider having access to a specific resources hierarchy for backup storage assigned exclusively to a dedicated ICT team that does not normally work with the production resources hierarchy or with the DRP resources hierarchy. And apply trustworthiness tests at every stage of the engagement.

For more details, see: Organizational Coping in Cyber Space: The Insider Threat - Defense Recommendations[85]

7. **Retention Lock -** define that backed up data cannot be deleted and/or modified for a period of X days by using a mechanism that locks an archive and/or by adopting other accepted methods in a public cloud.
8. **Backup versions management -** define versions for backed up data, so that a rollback is possible, should the need arise.
9. **Frequent backups** (for example: continuous and ongoing backups) **-** speed up recovery times and increase the efficiency of recovery from ransomware incidents. Backups that are several weeks or several months old are significantly less capable of coping than backups performed on a frequent basis.
10. **Characterization of the content to be backed up -** advance characterization of the types of data to be backed up helps coping efforts after an attack has shut down the online storage. While file storage is important, backing up of configuration settings, databases, and other types of data is also vital, even if not intuitive.
11. **File Versioning -** a simpler and more accessible solution, but at the same time less comprehensive, which preserves previous versions of all the files. Thus, if the files are modified, previous versions of them can be restored. Note that file versioning does not provide a sufficiently comprehensive solution for securing all the CSCs data types, and is unlikely to prevent an attacker who gained access to the authentication details of a legitimate user from executing uncontrolled changes, such as deleting data. Especially in cases where the CSC defined that disabling file versioning requires successful multifactor authentication (MFA).

[85] Organizational Coping in Cyber Space: The Insider Threat - Defense Recommendations, the Israel National Cyber Directorate, February 2019
https://www.gov.il/en/pages/coping_thret

A common error among CSCs is their basic assumption that the CSP is responsible for backups of the organizational data. This is all the more so when CSCs use a SaaS platform. In the light of this, it should be made clear that as a rule the CSP is not responsible for backups, and that backups are the CSCs full responsibility, unless the contractual engagement between the parties stipulates otherwise. In any event, the CSC should itself periodically validate the backups in order to make sure that the CSC can use them should the need arise.

For more details, see: Cloud Backup Security[86]

Incorporation of cyber defense principles in backups and restores[87]

Data replication

Data in one CSC environment can be replicated to another CSCs environment. It is good practice to adopt the following:

1. **Asynchronous replication** - use of asynchronous replication increases the likelihood that in the event that the data in one copy is encrypted, another copy of the existing data at the CSCs disposal will not be encrypted immediately. The time window until the asynchronous replication is completed enables the CSC to detect the attack and to implement disaster recovery more effectively and efficiently.
2. **Replication to another region or to another CSP** - replication to another region and/or to another CSP can be of considerable assistance when a CSP infrastructure vulnerability is exploited that enables an attacker to corrupt or delete data laterally.
3. **Use of file versioning** - similar to that mentioned above.

[86] Cloud Backup Security
https://www.gov.il/he/pages/alert_1795

[87] Incorporation of the cyber defense principles in backups and restores, the Israel National Cyber Directorate, February 2021
https://www.gov.il/he/pages/backup_restore

DETECT category

Detection and analysis of cyber attacks and anomalies.

Continuous Monitoring (DE.CM)

Sources of telemetry for cyber monitoring purposes

As part of the preparedness for cyber incidents and examination of the security posture, sources from which telemetry is to be collected should be defined in advance. It is good practice to integrate third-party tools such as CSPM (SSPM in the event of SaaS platform monitoring) and DSPM to complete the coverage.

Cloud providers generally allow transfer of data in an event and/or log configuration. Data transfer in an event configuration is usually near real-time, but the data quantity is limited. Conversely, data transfer in a log is slower, but much more comprehensive, essential for an optimal investigation.

Which events and logs are relevant should be defined in advance in relation to the risk profile. Without their operation in advance, an effective investigation after the event is generally not possible, making it really difficult to conduct damage control, attack vector detection, etc. Note that the Privacy Protection Authority has published a Guide to Implementing Regulation 10 of the Data Security Regulations - Saving Documentation and Logs [88].

As a rule of thumb, the definitions should be applied as set out in the official documentation of the relevant cloud provider, such as the Well-Architected Framework and the Cloud Adoption Framework.

The following table presents common sources of telemetry in a public cloud:

[88] New Guide to Implementation of Regulation 10 of the Data Security Regulations - Saving Documentation and Logs, the Privacy Protection Authority, September 29, 2024
https://www.gov.il/he/pages/takana10d

Management Plane Logs	Service Logs	Resource Logs	Cloud Tools
• Critical source given the importance of protecting the management plane.	• API Gateway: Access logs • Storage: Access logs • Network: VPC Flow logs • Function/Serverless: Activity logs • Cloud load balancer: Activity logs • Cloud DNS: Query logs • Cloud WAF/Firewall: Activity logs	• Workload: Instance, VM logs • Configuration change logs • Cloud function invocation logs • Database transaction logs • Object storage file access logs • Snapshot and image logs (block storage)	• CSPM (Cloud Security Posture Management - SPM) • CASB (Cloud Access Security Broker) • CNAPP (Cloud Native Application Protection Platform) • SSPM (SaaS SPM) • DSPM (Data SPM) • IAM analytics • Cloud detection and response

89

Table 8: Typical sources for collecting telemetry on cloud platforms

The data collected from the various telemetry sources should be transferred as quickly as possible to a data lake or to an SIEM system, which could thwart the attacker's efforts to compromise the CSCs capacity to investigate and detect adverse events. The data produced from the telemetry sources should be saved for a period of at least one year. Bear in mind that the requirements and regulations may call for the CSC [90]to save the data for an even longer period.

In addition to the list of sources above, sources containing FinOps data must also be addressed.

Consideration must be given to the fact that many logs in a cloud environment are not enabled by default. For example: DNS and Flow Logs.

In the light of this, the types of logs needed to monitor and respond to information and cyber incidents must be defined in advance, and action taken to verify that they are produced by the various assets and transferred to a data lake or SIEM system.

[89] Security Guidance for Critical Areas of Focus in Cloud Computing v5, CSA, July 15, 2024 https://cloudsecurityalliance.org/artifacts/security-guidance-v5

[90] See also, for example: Protection of Privacy Regulations (Data Security), 5777-2017; the Archives Law, 5715-1955; National Health Regulations (Saving Records), 5736-1976; and regulatory directives

Detection as Code

Detection as Code is a strategic approach that incorporates built-in information security and cybersecurity mechanisms for detection purposes in the software development lifecycle. By treating security control as code, organizations can automate the layout, management of the configuration settings, and maintenance of the security measures throughout the development process. This approach is aligned with the DevSecOps concept, which integrates information security and cybersecurity into the development process, instead of treating it as a separate, independent stage. As a function of this, organizations can develop advanced detection capabilities (such as rules, heuristics and machine learning models to detect anomalies), while adopting DevSecOps principles that reduce the need for manual testing, thereby speeding up development and integration of new security capabilities.

Adverse event analysis (DE.AE)

Analysis of adverse events in a public cloud includes characteristics similar to those that in on-premises organizational infrastructures, but also includes characteristics unique to this environment.

Below are several key recommendations for adverse event analysis in a public cloud environment:

1. The rate of alerts, and the scale and variety of the logs should be significantly greater than for on-premises organizational infrastructures.
2. Mostly, the transfer rate for logs from the resources to the monitoring system is less than for alerts. Therefore, the CSC must prepare in advance to contend with the time gap until the logs arrive at the monitoring system, which sometimes requires analysis and drawing of conclusions while information is still lacking.
3. Monitoring, identity management, authentication and access control constitute a challenge of the first order when working in a hybrid cloud configuration, as well as in a multi-cloud environment. It must therefore be verified that the CSC has

the practices, technologies, and personnel capable of responding adequately to this challenge.

4. In order to normalize the data received, advance steps should be taken, such as building a connector and configuring the schema mapping. This issue creates a significant challenge, especially when working in a multi-cloud configuration.
5. Continuous analysis of the attack surface and configuration settings is required. It is common for misconfigurations in cloud environments to serve as an attack vector that is easily exploited by attackers.
6. Continuous monitoring of file trustworthiness and integrity is recommended, including detecting of anomalies and changes in file entropy levels compared to previous levels, obscure changes in file extensions, and presence of known malware in files.
7. Monitor all the infrastructure components, even those that are not normally used. For example: detecting the adding and running of a new function in a serverless architecture. And in the case of a SaaS platform, configuring a new backup process or adding a new destination for saving a backup to.
8. Use artificial intelligence (AI) for information security and cybersecurity, including a decision support tool, in accordance with the organizational AI usage policy.
9. Incorporate a SOAR solution to build playbooks (triggers /events/ responses) in order to minimize the need for human intervention. In this context, build a Malware Investigation Pipeline to automate testing.
10. Correlation with CTI sources can help provide a rapid response to known threats and achieve situational awareness.
11. The duration of the anomaly detection and analysis must be as short as possible. Just a few seconds at most.

Note that even in cases where the CSC has limited resources preventing it from purchasing advanced tools, adverse events can be detected using relatively simple measures, such as:

1. Detecting a communications anomaly on the basis of exceptional traffic volumes.

2. Detecting an anomaly in the financial consumption of CSP services. The information security and cybersecurity team should integrate the FinOps officer in this activity.
3. Detecting anomalous create/ read/ update/ delete (CRUD) operations. Such as a user who modifies more than an X number of files in an hour.
4. Detecting changes in data backup and storage processes.
5. Detecting the setting up of new user accounts or multiple failed login attempts.
6. Resources initiate Internet activity that have no business need to do so.
7. End-user stations initiate traffic outside regular work hours at any site/ in any country the CSCS employees work in.
8. Detecting access of assets/ to assets from IP addresses or domains with a poor reputation (such as IP addresses that belong to well-known attack campaigns/ adversary and enemy infrastructures, or IP addresses associated with proxy services).
9. Use of the cloud native security capabilities, such as defining that sensitive information in a resource written in clear text (such as secrets and PII/ PHI) will generate an alert to the information security and cybersecurity team.

Examining the maturity level of the SOC system

It is good practice to use a SOC-CMM[91] model to examine the maturity level of the SOC system. The public cloud should only be utilized once the CSC or an entity acting on its behalf (such as an MDR) has achieved at least SOC-CMM Level 4 maturity (Quantitatively Managed) and Level 4 capability (Managed), and has maintained this levels for a reasonable duration.

RESPOND category

Actions taken when a cyber incident is identified.

[91]SOC-CMM
https://www.soc-cmm.com/

Incident management (RS.MA)

Incident response readiness (IR Readiness) is vital given that the CSC is liable to encounter a cloud cyber incident at some point in time. It is good practice for the CSC to adopt the following steps:

1. Verify that the cloud environment has been designed in accordance with the NIST Cloud Computing Forensic Reference Architecture[92].
2. Activate the appropriate telemetry sources in advance, including conveyance of alerts and logs to a centralized SIEM or to a data lake.
3. Verify that the CSC possesses the skills and tools necessary for the effective and efficient management of cloud IR processes.
4. Verify that the CSC has an architecture diagram and up-to-date mapping of the assets according to their level of criticality/ sensitivity.
5. Conduct periodic cloud IR exercises, and incorporate relevant partners, such as an IR company.
6. Verify the existence of a contractual agreement with the CSP, including the possibility of using its IR team according to a clearly worded service level agreement (SLA).
7. Make sure that an intra-organizational operational-level agreement (OLA) is defined for receipt of assistance from the relevant parties in the CSC.
8. Verify that the CSC has an alternative means of payment to purchase services from the CSP that it normally works with, or from an alternative CSP should the need arise.
9. Verify that the CSC has a dedicated environment (such as a dedicated deployment environment), in which DFIR means have been installed in advance as part of cyber incident readiness.
10. Verify that the CSC has the knowledge and ability to make optimal use of the CSPs eDiscovery service.

[92] NIST SP 800-201 - NIST Cloud Computing Forensic Reference Architecture, NIST, July, 2024 https://csrc.nist.gov/pubs/sp/800/201/final

11. Verify that special user accounts are defined for the purposes of incident management and digital forensics.
12. If necessary, verify that access permissions granted for a Cross-Deployments Role apply accepted principles, such as Least Privilege, Need to Know and Need to See, SoD.
13. Just-in Time Admin - achieved by a Just-in Time Admin mechanism and STS token, restricting access exclusively to the assets relevant to the investigation.
14. In the case of ephemeral assets (such as a container), verify in advance that the asset sends all the relevant logs to the monitoring system before it is deleted or shut down. Otherwise, when the asset is deleted or shut down, the CSC may lose data of investigative value.
15. Tagging of resources that need to be investigated and subjected to forensics, for optimal control and documentation of the IR process. An example of tagging: Forensics_Date.
16. Verify that the security policies applied to cloud resources (e.g., Service Control Policies) do not impede the ability to perform DFIR processes optimally.

If necessary, the CSC can use an external IR company; in that case too, the company must be well-acquainted with the environment, and conduct periodic joint exercises with the CSC. An SLA should be concluded with the IR company as well. The SLA must address extreme situations clearly, such as an incident that impacts multiple customers of the IR company simultaneously.

Verify that the response plan includes reference to cases in which a cyber incident starts in the CSCs public cloud environment and then leaps to on-premises organizational infrastructures and/or to another of the CSCs cloud environments, and the reverse.

Experience dictates that to preserve high levels of competency and readiness, the CSC must conduct frequent exercises to hone its ability to build a multidimensional investigative timeline when this type of incident occurs, including gathering of

artifacts from a large number of sources, while adhering to the chain of evidence principle.

Reporting and communication during an incident (RS.CO)

Verify that the CSC has a systematic process for reporting and communicating during an cyber incident. The following are several important recommendations in this regard:

1. Periodically map whether the duty to report to one or more regulators exists in the country the CSC operates in. See also Data Breach Notification Laws.
2. Periodically map whether there is a duty to report to one or more regulators in the country in which the CSCs data is stored and/or processed.
3. Notify the CSP when a cyber incident occurs, because the contractual agreement often grants the CSP the option of blocking the CSCs operations in the event of anomalies and/or concerns about a third party being harmed.
4. Verify that the CSC has an alternative communications channel for managing a cyber incident, so that if an attacker gains a hold, it will still be possible to yield information and to communicate in a manner that makes incident handling activities possible.

Mitigating the impact of the cyber incident (RS.MI)

Below are several key recommendations for mitigating the impact of a cyber incident in a public cloud environment:

1. In a public cloud, there is usually no need to "repair" assets that were adversely impacted, such as a virtual machine or a container, for example. Instead, one copy of the adversely impacted assets can be set aside for investigation, and another "clean copy" initialized in a "clean environment" using IaC or other acceptable method.
2. Incorporate a SOAR solution to build playbooks (triggers /events/ responses) in order to minimize the need for human intervention. In the absence of resources

to purchase a SOAR solution, you can use functions in a serverless architecture in order to execute basic responses, such as disconnecting an adversely impacted asset from the production environment or sending a message to the information security and cybersecurity team.

3. Public cloud native tools enable deployment of corrective control with respect to on-premises organizational infrastructures within a relatively short time.

In a cyber incident, the CSC or parties representing it may use online investigation services, such as a special testing environment (sandbox). Address the consequences of exposing the organizational data to such services, which might violate privacy and/or intellectual property, or expose the existence of the investigation to the attacker.

RECOVER category

Restoring assets and processes harmed as a result of a cyber incident.

Implementation of an incident recovery plan (RC.RP)

It is vital that the business continuity plan and the disaster recovery plan include reference to work in the cloud, and address the special challenges posed by this environment. The CSC should periodically, and at least once a year, conduct an exercise of its ability to set up a complete environment from scratch and continue business operations from this environment for at least ten calendar days.

Communications during incident recovery operations (RC.CO)

Relevant stakeholders should be updated periodically about the status of the recovery operations. Relevant stakeholders should also be allocated a personalized dashboard on the CSP management console so that they can directly monitor the status of the recovery operations.

For more details on cyber incident management, the following is recommended reading:

NIST SP 800-61 Rev. 3 (Initial Public Draft)
Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile[93]

Cloud Incident Response Framework, Cloud Security Alliance (CSA)[94]

Best Practices for Cyber Crisis Management, ENISA[95]

[93] NIST SP 800-61 Rev. 3 (Initial Public Draft)
Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST, April 3, 2024
https://csrc.nist.gov/pubs/sp/800/61/r3/ipdManagement: A CSF 2.0 Community Profile, NIST, April 3, 2024
https://csrc.nist.gov/pubs/sp/800/61/r3/ipd
[94] Cloud Incident Response Framework, CSA, April 05, 2021
https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework
[95] Best Practices for Cyber Crisis Management, ENISA, February 28, 2024
https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

Checklist

This section presents a checklist of the risk mitigation methods appearing in this document.

No.	Category name	Subcategory name	Application status
1.	GOVERN	Risk management strategy (GV.RM)	
2.		Policy (GV.PO)	
3.		Supply chain security (GV.SC)	
4.	IDENTIFY	Asset management (ID.AM)	
5.		Risk assessment (ID.RA)	
6.		Striving for continuous improvement (ID.IM)	
7.	PROTECT	Identity management, authentication, and access control (PR.AA)	
8.		Awareness and training (PR.AT)	
9.		Data security (PR.DS)	
10.		Platform security (PR.PS)	
11.		Technology infrastructure resilience (PR.IR)	
12.	DETECT	Continuous monitoring (DE.CM)	
13.		Adverse event analysis (DE.AE)	
14.	RESPOND	Incident management (RS.MA)	
15.		Incident response reporting and communication (RS.CO)	
16.	RECOVER	Implementation of an incident recovery plan (RC.RP)	
17.		Communications during incident recovery operations (RC.CO)	

Table 9: Checklist of the risk mitigation methods contained in this document

Acronyms

This section presents a list of the acronyms used in this document.

No.	Acronym	Term
1.	2SV	Two Step Verification
2.	A2A	Application-to-Application
3.	A2P	Application-to-Person
4.	ACL	Access Control List
5.	AD	Active Directory
6.	ADFS	Active Directory Federation Services
7.	AI	Artificial Intelligence
8.	AIBOM	AI Bill of Materials
9.	AIMS	Artificial Intelligence Management System
10.	AITM	Adversary-in-the-Middle
11.	API	Application Programing Interface
12.	ASPM	Application Security Posture Management
13.	AS-REP	Authentication Server Response
14.	ASVS	Application Security Verification Standard
15.	ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
16.	AWS	Amazon Web Services
17.	BCP	Business Continues Process
18.	BIA	Business Impact Analysis
19.	BIMI	Brand Indicator for Message Identification
20.	BYOD	Bring Your Own Device
21.	C2	Command & Control

No.	Acronym	Term
22.	CAF	Cloud Adoption Framework
23.	CD	Continuous Delivery
24.	CDN	Content Delivery Network
25.	CDR	Content Disarm & Reconstruction
26.	CI	Continuous Integration
27.	CIEM	Cloud Infrastructure Entitlement Management
28.	CIS	Center for Internet Security
29.	CISA	The Cybersecurity and Infrastructure Security Agency
30.	CLI	Command Line Interface
31.	CMM	Capability Maturity Model
32.	CNAPP	Cloud-Native Application Protection Platform
33.	CPU	Central Processing Unit
34.	CRUD	Create, Read, Update, and Delete
35.	CS	Certificate Services
36.	CSA	Cloud Security Alliance
37.	CSC	Cloud Service Customer
38.	CSP	Cloud Service Provider
39.	CSPM	Cloud Security Posture Management
40.	CTI	Cyber Threat Intelligence
41.	CWPP	Cloud Workload Protection Platform (CWPP)
42.	D3FEND	Detection, Denial, and Disruption Framework Empowering Network Defense
43.	DAST	Dynamic Application Security Testing
44.	DC	Domain Controller
45.	DDoS	Distributed Denial-of-Service

No.	Acronym	Term
46.	DevOps	Development (Dev) and Operations (Ops)
47.	DevSecOps	Development, Operations and Security
48.	DFIR	Digital Forensics and Incident Response
49.	DISA	The Defense Information Systems Agency
50.	DLP	Data Leak Prevention
51.	DMARC	Domain-based Message Authentication, Reporting & Conformance
52.	DNS	Domain Naming Server
53.	DOC	Detection-as-Code
54.	DoW	Denial-of-Wallet
55.	DPO	Data Protection Officer
56.	DR	Disaster Recovery
57.	DRP	Disaster Recovery Plan
58.	DSPM	Data Security Posture Management
59.	EBS	Elastic Block Store
60.	eDiscovery	Electronic Discovery
61.	EDoS	Economic Denial of Sustainability
62.	EMM	Enterprise Mobility Management
63.	ENISA	The European Union Agency for Cybersecurity
64.	FedRAMP	The Federal Risk and Authorization Management Program
65.	FIDO	Fast Identity Online
66.	FIM	File Integrity Monitoring
67.	FinOps	Financial Operations
68.	FIPS	Federal Information Processing Standards
69.	GCP	Google Cloud Platform

No.	Acronym	Term
70.	GenAI	Generative AI
71.	GRC	Governance, Risk Management, and Compliance
72.	GW	Gateway
73.	H2M	Human to Machine
74.	HSM	Hardware Security Module
75.	IaaS	Infrastructure as a Service
76.	IaC	Infrastructure as a Code
77.	IAM	Identity and Access Management
78.	IAST	Interactive Application Security Testing
79.	ICT	Information and Communications Technology
80.	IdP	Identity Provider
81.	IEC	International Electrotechnical Commission
82.	IMDS	Cloud Instance Metadata Services
83.	IPFS	The InterPlanetary File System
84.	ISO	International Organization for Standardization
85.	IT	Information Technology
86.	JSON	JavaScript Object Notation
87.	JWT	JSON Web Tokens
88.	KCI	Key Control Indicators
89.	KGI	Key Goal Indicator
90.	KMS	Key Management Server
91.	KPI	Key Performance Indicator
92.	KRI	Key Risk Indicator
93.	LAN	Local-Area Network

No.	Acronym	Term
94.	LB	Load Balancer
95.	LDAP	Lightweight Directory Access Protocol
96.	LLMNR	Local Loop Multicast Name Resolution
97.	LOTC	Living Off the Cloud
98.	LOTL	Living Off the Land
99.	LOTS	Living Off Trusted Sites
100.	M2M	Machine to Machine
101.	MASVS	Mobile Application Security Verification Standard
102.	MDM	Mobile Device Management
103.	MDR	Managed Detection and Response
104.	MFA	Multi-Factor Authentication
105.	ML	Machine Learning
106.	mTLS	Mutual TLS
107.	NBT-NS	NetBIOS over TCP/IP
108.	NGFW	Next Generation Firewall
109.	NIS	New Israeli Shekel
110.	NIST	National Institute of Standards and Technology
111.	NSG	Network Service Group
112.	NTLM	NT LAN Manager
113.	OCI	Oracle Cloud Infrastructure
114.	OCR	Optical Character Recognition
115.	OKR	Objective and Key Result
116.	OLA	Organization Level Agreement
117.	OSV	Open Source Vulnerabilities

No.	Acronym	Term
118.	OWASP	The Open Web Application Security Project
119.	P2P	Point to Point
120.	PaaS	Platform as a Service
121.	PAM	Privileged Access Management
122.	PET	Privacy-Enhancing Technologies
123.	PHI	Protected Health Information
124.	PIA	Privacy Impact Assessment
125.	PII	Personal Identifiable Information
126.	PIM	Privileged Identity Management
127.	PtH	Pass-the-Hash (PtH)
128.	PtT	Pass-the-Ticket (PtT)
129.	QR	Quick Response Code
130.	RASP	Runtime Application Self-Protection
131.	RBAC	Role-Based Access Control
132.	RBI	Remote Browser Isolation
133.	RCE	Remote Code Execution
134.	RCP	Resource Control Policy
135.	RDDoS	Ransom DDoS
136.	RDP	Remote Desktop Protocol
137.	RMF	Risk Management Framework
138.	RMM	Remote Monitoring and Management
139.	RPO	Recovery Point Objectives
140.	RTO	Recovery Time Objectives
141.	S2S	Site to Site

No.	Acronym	Term
142.	S3	Simple Storage Service
143.	SaaS	Software as a Service
144.	SaaSBOM	Software-as-a-Service BOM
145.	SAML	Security Assertion Markup Language
146.	SASE	Secure Access Service Edge
147.	SAST	Static Application Security Testing
148.	SBOM	Software Bill of Materials
149.	SCA	Software Composition Analysis
150.	SCIM	System for Cross-domain Identity Management
151.	SCM	Source Code Management
152.	SCP	Service Control Policy
153.	SDK	Software Development Kit
154.	SID	Security Identifier
155.	SIEM	Security Information and Event Management,
156.	SLA	Service Level Agreement
157.	SNMP	Simple Network Management Protocol
158.	SOAR	Security Orchestration, Automation, and Response
159.	SOC	Security Operations Center
160.	SoD	Separation of Duties
161.	SP	Special Publications
162.	SRM	Shared Responsibility Model
163.	SSDF	Secure Software Development Framework
164.	SSH	Secure Shell
165.	SSM	Systems Manager

No.	Acronym	Term
166.	SSO	Single-Sign On
167.	SSPM	SaaS Security Posture Management
168.	SSRF	Server-Side Request Forgery
169.	STAR	The Security Trust Assurance and Risk
170.	STIG	Security Technical Implementation Guides
171.	STS	Security Token Service
172.	TCP/IP	Transmission Control Protocol/Internet Protocol
173.	TLP	Traffic Light Protocol
174.	TLS	Transport Layer Security
175.	TTP	Tactics Techniques and Procedures
176.	UEBA	User and Entity Behavior Analytics
177.	URL	Uniform Resource Locator
178.	UX	User Experience
179.	VCN	Virtual Cloud Network
180.	VLAN	Virtual LAN
181.	VNeT	Virtual Network
182.	VPC	Virtual Private Cloud
183.	VPN	Virtual Private Network
184.	VXLAN	Virtual eXtensible Local-Area Network
185.	WAAP	Web Application and API Protection
186.	WAF	Web Application Firewall
187.	WMI	Windows Management Instrumentation
188.	WORM	Write Once Read Many
189.	WPAD	Web Proxy Auto-Discovery Protocol

Table 10: Acronyms and the terms

References

This section contains the main references that the authors based themselves on in writing this document.

Israel National Cyber Directorate publications

Cloud Backup Security, Israel National Cyber Directorate, August 29, 2024
https://www.gov.il/he/pages/alert_1795

The Economic Cost of Cyber Attacks in Israel: NIS 12 billion a year, the Israel National Cyber Directorate, April 2024
https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_5_2024

Cyber Exercise - Building and Conducting Organization Cyber Exercises, the Israel National Cyber Directorate, December 2022
https://www.gov.il/he/pages/cyberexercise

Exploitation of Software Dependencies for attacks, the Israel National Cyber Directorate, February 16, 2021
https://www.gov.il/he/pages/dependencies

Integration of Cyber Defense Principles in Backup and Restore Processes, the Israel National Cyber Directorate, February 2, 2021
https://www.gov.il/he/pages/backup_restore

Organizational Coping in Cyber Space: The Insider Threat - Defense Recommendations, the Israel National Cyber Directorate, February 2019
https://www.gov.il/he/pages/coping_thret

National Cyber Concept for Crisis Preparedness and Management, the Israel National Cyber Directorate, November 6, 2018
https://www.gov.il/he/pages/cybercrisispreparedness

Golden SAML - Expanding an Attack from the Organizational Network to the Cloud Resources, November 22, 2017
https://www.gov.il/BlobFolder/reports/saml/he/SAML-CERT-IL-W-365.pdf

Israel National Digital Agency publications

Cloud Risk Management, Compliance and Control (GRC) Document, the Israel National Digital Agency, January 21, 2024
https://www.gov.il/he/pages/grcnews

Government Cloud Operating Model - Processes and Organizational Change Aspects, the Israel National Digital Agency, November 23, 2023
https://www.gov.il/he/pages/operatingmodel_news

The Government Cloud Strategy, the Israel National Digital Agency, December 11, 2022
https://www.gov.il/he/pages/strategy_1

Privacy Protection Authority publications

New Guide to Implementation of Regulation 10 of the Data Security Regulations - Saving Documentation and Logs, the Privacy Protection Authority, September 29, 2024
https://www.gov.il/he/pages/takana10d

The Challenges in Migrating Databases and Database Systems to the Cloud, the Privacy Protection Authority, September 5, 2024

https://www.gov.il/he/pages/cloud_databases

Directive on the Role of the Board of Directors in upholding Corporate Duties in accordance with the Protection of Privacy Regulations (Data Security), the Privacy Protection Authority, September 3, 2024
https://www.gov.il/he/pages/the_board_role

Amendment 13 to the Protection of Privacy Law, August 14, 2024
An extensive amendment to the Protection of Privacy Law, the most comprehensive made to the Law since its enactment 43 years ago, which expands the enforcement tools and the powers of the Privacy Protection Authority
https://www.gov.il/he/pages/13_amendment

The Authority published a methodical help guide to conducting a privacy impact assessment - to help organizations in the economy assess and mitigate risks to privacy, the Privacy Protection Authority, November 23, 2022
https://www.gov.il/he/pages/taskir_privacy_news

Publications by other Government bodies in the State of Israel

Information technology risk management, information security and cyber protection (Directive No. 364), Supervisor of Banks, November 18, 2024
https://www.boi.org.il/roles/supervisionregulation/nbt/nbt364

Principles, Policy, Regulations and Ethics in the Area of Artificial Intelligence 2023, the Ministry of Innovation, Science and Technology, December 14, 2023
https://www.gov.il/he/pages/ai_23

Cloud computing (Directive No. 362), Supervisor of Banks, June 13, 2022
https://www.boi.org.il/roles/supervisionregulation/nbt/nbt362/

Publications by other government bodies abroad

Australia

Information Security Manual (ISM)
https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

Our Cloud Information Governance Policy
https://www.naa.gov.au/about-us/who-we-are/accountability-and-reporting/our-cloud-information-governance-policy

UK

G-Cloud 14
https://www.crowncommercial.gov.uk/agreements/RM1557.14

Cloud security guidance, NCSC
https://www.ncsc.gov.uk/collection/cloud

European Union

EU Cloud Certification Scheme
https://ec.europa.eu/newsroom/cipr/items/713799/en

Germany

Criteria catalogue C5
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

United States

Cloud Gov
https://cloud.gov

DoD Cloud Computing Security
https://public.cyber.mil/dccs/

The Federal Risk and Authorization Management Program (FedRAMP)
https://www.fedramp.gov

CISA Publications

CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices, CISA, March 07, 2024
https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices

Guide to Securing Remote Access Software, CISA, June 06, 2023
https://www.cisa.gov/resources-tools/resources/guide-securing-remote-access-software

Zero Trust Maturity Model, CISA, April, 2023
https://www.cisa.gov/zero-trust-maturity-model

Protecting Against Malicious Use of Remote Monitoring and Management Software, CISA, January 26, 2023

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a

CISA Releases JCDC Remote Monitoring and Management (RMM) Cyber Defense Plan, CISA, August 16, 2023
https://www.cisa.gov/news-events/alerts/2023/08/16/cisa-releases-jcdc-remote-monitoring-and-management-rmm-cyber-defense-plan

Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, CISA, April 15, 2021
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

Free Tools for Cloud Environments
https://www.cisa.gov/resources-tools/resources/free-tools-cloud-environments

Open Source Vulnerabilities (OSV)
https://www.cisa.gov/resources-tools/services/open-source-vulnerabilities-osv

Software Bill of Materials (SBOM)
https://www.cisa.gov/sbom

CISA #Stopransomware

https://www.cisa.gov/stopransomware

Cloud Security Alliance (CSA) publications

Zero Trust Guiding Principles v1.1, CSA, September 03, 2024
https://cloudsecurityalliance.org/artifacts/zero-trust-principles-v-1-1

Top Threats to Cloud Computing 2024, CSA, August 05, 2024
https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

AI Model Risk Management Framework, CSA, July 23, 2024
https://cloudsecurityalliance.org/artifacts/ai-model-risk-management-framework

Security Guidance for Critical Areas of Focus in Cloud Computing v5, CSA, July 15, 2024
https://cloudsecurityalliance.org/artifacts/security-guidance-v5

How to Design a Secure Serverless Architecture, CSA, October 23, 2023
https://cloudsecurityalliance.org/artifacts/how-to-design-a-secure-serverless-architecture

MOVEit Exploit & Ransomware Attack: Why SaaS Security Is Critical During a Cyberattack, CSA, August 11, 2023
https://cloudsecurityalliance.org/blog/2023/11/08/moveit-exploit-ransomware-attack-why-saas-security-is-critical-during-a-cyberattack

SaaS Governance Best Practices for Cloud Customers, CSA, October 10, 2022
https://cloudsecurityalliance.org/artifacts/saas-governance-best-practices-for-cloud-customers

SaaS Security and Misconfigurations Report, CSA, April 04, 2022
https://cloudsecurityalliance.org/artifacts/saas-security-and-misconfigurations-report

Cloud Incident Response Framework, CSA, April 05, 2021
https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework

ENISA publications

ENISA Threat Landscape 2024, ENISA, September 19, 2024
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Best Practices for Cyber Crisis Management, ENISA, February 28, 2024
https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

ISO Publications

ISO/IEC 27032:2023
Cybersecurity – Guidelines for Internet security

ISO/IEC 42001:2023
Information technology – Artificial intelligence – Management system
https://www.iso.org/standard/81230.html

ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection – Information security management systems – Requirements

ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection – Information security controls

ISO/IEC 27018:2019
Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27701:2019
Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

ISO/IEC 27017:2015
Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

MITRE publications

D3FEND Matrix
https://d3fend.mitre.org/

MITRE ATT@CK Framework
https://attack.mitre.org/

Threat Modeling with ATT&CK v1.0.0
https://center-for-threat-informed-defense.github.io/threat-modeling-with-attack/

MITRE ATLAS
https://atlas.mitre.org/

MITRE Engage
https://engage.mitre.org/

NIST publications

NIST SP 800-63-4 (2nd Public Draft) Digital Identity Guidelines, NIST, August 21, 2024
https://csrc.nist.gov/pubs/sp/800/63/4/2pd

NIST SP 800-201 - NIST Cloud Computing Forensic Reference Architecture, NIST, July, 2024
https://csrc.nist.gov/pubs/sp/800/201/final

NIST SP 800-61 Rev. 3 (Initial Public Draft)
Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST, April 3, 2024
https://csrc.nist.gov/pubs/sp/800/61/r3/ipd

NIST SP 1800-28
Data Confidentiality: Identifying and Protecting Assets Against Data Breaches, NIST, February, 2024
https://csrc.nist.gov/pubs/sp/1800/28/final

NIST Cybersecurity Framework (CSF) 2.0, NIST, February 26, 2024
https://www.nist.gov/cyberframework

NIST SP 800-82 Rev. 3
Guide to Operational Technology (OT) Security, NIST, September, 2023
https://csrc.nist.gov/pubs/sp/800/82/r3/final

NIST AI RMF Playbook, NIST, March 30, 2023
https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook

NIST AI RMF v1.0, NIST, January 2023
https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development

NIST SP 800-160 Vol. 1 Rev. 1 Engineering Trustworthy Secure Systems, NIST, November, 2022
https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

NIST IR 8374, NIST
Ransomware Risk Management: A Cybersecurity Framework Profile, NIST, February, 2022
https://csrc.nist.gov/pubs/ir/8374/final

NIST SP 800-218
Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST, February, 2022
https://csrc.nist.gov/pubs/sp/800/218/final

NIST SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST, December, 2021
https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

NIST SP 1800-25, NIST
Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, NIST, December, 2020
https://csrc.nist.gov/pubs/sp/1800/25/final

NIST SP 1800-11 Series - Data Integrity: Recovering from Ransomware and Other Destructive Events, NIST, September, 2020
https://www.nccoe.nist.gov/data-integrity-recovering-ransomware-and-other-destructive-events

NIST SP 800-53 Rev. 5
Security and Privacy Controls for Information Systems and Organizations, NIST, September, 2020
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NISTIR 8006, NIST Cloud Forensic Science Challenges, NIST, August, 2020
https://csrc.nist.gov/Projects/cloud-forensics

NIST SP 800-145 - The NIST Definition of Cloud Computing, NIST, September, 2011
https://csrc.nist.gov/pubs/sp/800/145/final

NIST Cloud Computing Reference Architecture, NIST, September 8, 2011
https://www.nist.gov/publications/nist-cloud-computing-reference-architecture

OWASP publications

OWASP Top 10 Risks for Open Source Software
https://owasp.org/www-project-open-source-software-top-10/

OWASP Top 10 CI/CD Security Risks
https://owasp.org/www-project-top-10-ci-cd-security-risks/

OWASP Top 10 Proactive Controls
https://top10proactive.owasp.org/

OWASP Application Security Verification Standard (ASVS)
https://owasp.org/www-project-application-security-verification-standard/

OWASP MASVS (Mobile Application Security Verification Standard)
https://mas.owasp.org/MASVS/

OWASP Top 10 API Security Risks
https://owasp.org/www-project-api-security/

OWASP Top 10 Risks for Open Source Software
https://owasp.org/www-project-open-source-software-top-10/

OWASP Top 10 CI/CD Security Risks
https://owasp.org/www-project-top-10-ci-cd-security-risks/

OWASP Top 10 Proactive Controls
https://top10proactive.owasp.org/

OWASP Cloud-Native Application Security Top 10
https://owasp.org/www-project-cloud-native-application-security-top-10/

SANS publications

SANS Cloud Security Exchange 2024 eBook - Cloud Security: First Principles and Future Opportunities, SANS, August 23, 2024
https://www.sans.org/white-papers/cloud-security-first-principles-future-opportunities/

How the Cloud Changes SecOps and Incident Response: Lessons from a Real-World Living-Off-The-Cloud Attack, SANS, 15 Nov, 2023
https://www.sans.org/webcasts/how-the-cloud-changes-secops-and-incident-response-lessons-from-a-real-world-living-off-the-cloud-attack/

Cybersecurity in the Age of the Cloud, SANS, February, 2020
https://www.sans.org/media/cloud-security/eBook_cloud-security.pdf

Incident Management 101 Preparation and Initial Response (aka Identification), SANS, January 17, 2005
https://www.sans.org/white-papers/1516/

Publications by well-known public cloud providers

Amazon Web Services (AWS)

AWS Cloud Adoption Framework (AWS CAF)
https://aws.amazon.com/cloud-adoption-framework/

Protecting against ransomware
Mitigate ransomware for your organization with AWS
https://aws.amazon.com/security/protecting-against-ransomware/

Design SaaS on AWS
https://aws.amazon.com/saas/design/

The confused deputy problem
https://docs.aws.amazon.com/IAM/latest/UserGuide/confused-deputy.html

Microsoft Azure

Microsoft Cloud Adoption Framework for Azure
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/

Ransomware protection in Azure
https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-protection

ENISA Information Assurance Framework
https://learn.microsoft.com/en-us/compliance/regulatory/offering-enisa

How to use policies to restrict where EC2 instance credentials can be used from
https://aws.amazon.com/blogs/security/how-to-use-policies-to-restrict-where-ec2-instance-credentials-can-be-used-from/

Google Cloud Platform (GCP)

Google Cloud Adoption Framework
https://cloud.google.com/adoption-framework

Best practices for mitigating ransomware attacks using Google Cloud
https://cloud.google.com/architecture/bps-for-mitigating-ransomware-attacks

Standardizing Privileged Access Architecture for Multi-Cloud v1.0
https://services.google.com/fh/files/misc/standardizing-privileged-access-architecture-for-multi-cloud.pdf

Oracle Cloud Infrastructure (OCI)

Cloud Adoption Framework for Oracle Cloud Infrastructure (OCI)
https://www.oracle.com/cloud/cloud-adoption-framework/

CISO Perspectives: Advanced Cyber-Resilience in OCI - Protecting your Tenancy Against Ransomware Style Threats
https://www.ateam-oracle.com/post/ciso-perspectives-protecting-your-oci-tenancy-against-ransomware-attacks

Oracle Cloud Infrastructure (OCI) Security Best Practices
https://docs.oracle.com/en-us/iaas/Content/Security/Reference/configuration_security.htm

Publications by various bodies

Securing AWS Lambda | How Misconfigurations Can Lead to Lateral Movement, Sentinel One, November, 2024
https://www.sentinelone.com/blog/lateral-movement-in-aws-lambda-environments/

AWS CDK Risk: Exploiting a Missing S3 Bucket Allowed Account Takeover, Aqua Security, October, 2024
https://www.aquasec.com/blog/aws-cdk-risk-exploiting-a-missing-s3-bucket-allowed-account-takeover/

Shuaib A Wadho, Sijjad Ali, Asma Ahmed A. Mohammed, Aun Yichiet, Ming Lee Gan and Chen Kang Lee, “Secret Sharing as a Defense Mechanism for Ransomware in Cloud Storage Systems” International Journal of Advanced Computer Science and Applications(IJACSA), 15(10), 2024.
http://dx.doi.org/10.14569/IJACSA.2024.01510102

2024 Cloud Native Security Report, Linux Foundation, October, 2024
https://www.linuxfoundation.org/research/cloud-native-security

Information Risk Insights Study RANSOMWARE, Cyentia Institute, 2024
A Detailed Analysis of the Frequency and Impact of Ransomware Events
https://www.cyentia.com/iris-ransomware/

The state of security in cloud native development 2024

https://www.cncf.io/blog/2024/09/26/the-state-of-security-in-cloud-native-development-2024/

Best Practices for Cloud Ransomware Protection in 2024
https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-ransomware-protection/

Living Off the Land Cloud (LOLCloud)
https://lolcloud-project.github.io/index.html

Navigating the New Cloud Security Landscape
https://www.clouddatainsights.com/navigating-the-new-cloud-security-landscape/

New Mamba 2FA bypass service targets Microsoft 365 accounts
https://www.bleepingcomputer.com/news/security/new-mamba-2fa-bypass-service-targets-microsoft-365-accounts/

Using honeytokens to detect (AiTM) phishing attacks on your Microsoft 365 tenant
https://zolder.io/blog/using-honeytokens-to-detect-aitm-phishing-attacks-on-your-microsoft-365-tenant/

How to protect against AiTM/Evilginx phishing attacks
https://cognisys.co.uk/blog/how-to-protect-against-aitm-evilginx-phishing-attacks/

X-Force report reveals top cloud threats: AITM phishing, business email compromise, credential harvesting and theft
https://www.ibm.com/blog/x-force-cloud-threat-landscape/

Best Practices for Securing Active Directory
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Amazon Web Services (AWS) Data Breaches: Full Timeline Through 2023
https://firewalltimes.com/amazon-data-breach-timeline/

Ransomware in the Cloud: Breaking Down the Attack Vectors
https://www.paloaltonetworks.com/blog/prisma-cloud/ransomware-data-protection-cloud/

Cloud Governance - Definition, Framework, and Principles
https://www.tatacommunications.com/knowledge-base/cloud-governance/

The Global State of CPS Security 2024: Business Impact of Disruptions
https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions
Cyberattacks and Security of Cloud Computing: A Complete Guideline

https://www.mdpi.com/2073-8994/15/11/1981

Detecting and mitigating Active Directory compromises
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/detecting-and-mitigating-active-directory-compromises

HackTricks
https://book.hacktricks.xyz/

Incident Response in Google Cloud: Forensic Artifacts
https://www.sygnia.co/blog/gcp-incident-response/

Announcing 'Cirrus' - New Opensource Tool to Combat Google Cloud Incident Response Challenges
https://www.sygnia.co/blog/new-opensource-tool-to-combat-google-cloud-incident-response-challenges/

SaaS attack techniques
https://github.com/pushsecurity/saas-attacks

Economic denial of sustainability (EDoS) mitigation approaches in cloud: Analysis and open challenges
https://ieeexplore.ieee.org/document/8167135

Multi-Cloud Security: Key Challenges and Effective Practices from Experts
https://www.techmagic.co/blog/multi-cloud-security

Public Cloud Security Breaches
https://www.breaches.cloud/

***** End of document *****