ETSI TR 103 959 V1.1.1 (2024-07)

TECHNICAL REPORT

Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Cloud Sector

Reference

DTR/CYBER-00109

Keywords

cloud computing, cyber security, cyber-defence,
data centres, information assurance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to
the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or
other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Cloud data centres, including cloud edge architectures, have become pervasive worldwide as a critical infrastructure sector for providing network ICT services and applications. The protection of this infrastructure from cyber security threats by instituting effective risk control and enhanced resilience has received the global attention of governmental authorities and industry organizations [i.1] to [i.19]. The present document addresses this protection challenge by providing guidance on individually applying the most current version of the Critical Security Controls for effective cyber defence [i.20] to cloud infrastructure. For compliance purposes, the Critical Security Controls have mappings to almost every known government and industry cyber security framework with extensive implementations for diverse operating systems and applications [i.22] and [i.23]. Included in the present document is a mapping to Cloud Security Alliance Security Controls framework together with an enumeration of known Cloud Data Centre OS Hardened Image implementations.

Introduction

The Critical Security Controls are a prioritized set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks. Under the auspices of the Center for Internet Security (CIS), the Controls are developed by a community of Information Technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the Controls come from a wide range of sectors including, retail, manufacturing, healthcare, education, government, defence, and others. While the Controls address the general practices that most enterprises should take to secure their systems, some operational environments may present unique requirements not addressed by the Controls.

The Controls started as a grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and share that information to help enterprises focus their attention on the most fundamental steps they should take to defend themselves. As the Controls continue to be refined and re-worked through the expert community, the need for Controls guidance for the cloud sector became clear [i.25], [i.27] and [i.31].

1 Scope

The present document applies the latest version of the Critical Security Controls [i.20] for effective risk control and enhanced resilience of the Cloud Sector and adds mappings to CSA Security Controls and Cloud Data Centre Hardened Image implementations [i.21].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).

[i.2] COM/2020/595 final: "Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014".

[i.3] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

[i.4] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[i.5] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance).

[i.6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

[i.7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[i.8] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[i.9] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the EU (NIS Directive).

[i.10] COM/2022/68 final: "Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)".

[i.11] COM/2012/0529 final: "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Unleashing the Potential of Cloud Computing in Europe".

[i.12] COM/2015/0192 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A digital single market strategy for Europe.

[i.13] COM/2016/0176 final: "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ICT Standardisation priorities for the digital single market".

[i.14] COM/2016/0178 final: "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Cloud Initiative - Building a competitive data and knowledge economy in Europe".

[i.15] COM/2021/118 final: "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade".

[i.16] National Cyber Security Centre: "Cloud security guidance".

[i.17] CISA Cybersecurity and Infrastructure Security Agency (Version 2.0): "Cloud Security Technical Reference Architecture".

[i.18] National Security Agency: "Mitigating Cloud Vulnerabilities".

[i.19] Cloud Security Alliance: "CSA Research Publications".

[i.20] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.21] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.22] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.23] ETSI TR 103 866: " Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.24] Cloud Security Alliance: "Cloud Controls Matrix (CCM)".

[i.25] Center for Internet Security: "Controls Cloud Companion Guide, V8".

[i.26] ENISA Cloud Security.

[i.27] ENISA: "EUCS - Cloud Services Scheme".

[i.28] EU CLOUD COC: "EU Cloud Code of Conduct".

[i.29] Center for Internet Security: "CIS Hardened Images® List".

[i.30] Center for Internet Security: "CIS Controls Mapping to Cloud Security Alliance Cloud Control Matrix".

[i.31] Center for Internet Security: "Shared Responsibility for Cloud Security: What You Need to Know".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

cloud sector: model that enables access to a shared pool of computing resources on-demand, and includes data centre, edge, and associated user hardware and software infrastructure

tokenization: process by which a piece of sensitive data, such as a credit card number, is replaced by a surrogate value known as a token

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization, and Auditing
API	Application Program Interface
CaaS	Containers as a Service
CASB	Cloud Access Security Broker
CCM	Cloud Controls Matrix
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CSA	Cloud Security Alliance
CSC	Critical Security Control
CSP	Cloud Service Provider
DevOp	Development and Operation
DevSecOp	Development, Security and Operation
DHCP	Dynamic Host Configuration Protocol
DMARC	Domain-based Message Authentication Reporting, and Conformance
DMZ	DeMilitarised Zone
DNS	Domain Name System
EUCS	European Union Cloud Security
FaaS	Function as a Service
HSM	Hardware Security Model
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
ICT	Information and Communications Technology
IDS	Intrusion Detection Systems
IG	Implementation Group
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
JSON	JavaScript Object Notation
MFA	Multifactor Authentication
OS	Operating System
OSCAL	Open Security Controls Assessment Language
OT	Operational Technology
PaaS	Platform as a Service
RBAC	Role-Based Access Control
SaaS	Software as a Service
SLA	Service-Level Agreements
SME	Small and Medium Enterprise
STAR	Security, Trust Assurance and Risk

TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network
YAML	YAML Ain't Markup Language

4 Applying the Critical Security Controls for effective risk control and enhanced resilience of the Cloud sector

4.1 Introduction, Methodology and Use

While many of the core security concerns of enterprise IT systems are shared within cloud environments, the main challenge in applying best practices is tied to the fact that these systems typically operate software and hardware under different assumed security responsibilities. Ensuring and understanding that the Service-Level Agreements (SLAs) and legal contracts with the Cloud Service Provider (CSP) highlight liability, service levels, breach disclosure, and incident response timeframes is an important piece of cloud security. The shared security responsibility, as well as the specific cloud services and deployment models utilized, changes who handles the security requirements and with whom the assumed security risk resides. CSPs are constantly adding new functional services along with configuration and security tools to better manage them at a very rapid pace. As new tools become available, the cloud consumer should consider a hybrid approach using third-party tools along with CSP native security tools that best fit an enterprise's security and management needs. Enterprise management processes should ensure there is overlap rather than gaps in coverage between native and third-party tools.

Cloud environments have service models that the applications or services can be classified under. These models have evolved over time and continue to emerge:

- **IaaS (Infrastructure as a Service)** is a cloud environment providing computing resources such as virtual servers, storage, and networking hardware. The consumer utilizes their own software such as operating systems, middleware, and applications. The underlying cloud infrastructure is managed by the CSP.

- **PaaS (Platform as a Service)** is a cloud computing environment for development and management of a consumer's applications. It includes the infrastructure hardware: virtual servers, storage, and networking while tying in the middleware and development tools to allow the consumer to deploy their applications. It is designed to support the complete application lifecycle while leaving the management of the underlying infrastructure to the CSP. In practice, there can be some IaaS/PaaS overlap (or, indeed, PaaS/SaaS).

- **SaaS (Software as a Service)** is a cloud computing software solution that provides the consumer with access to a complete software product. The software application resides on a cloud environment and is accessed by the consumer through the web or an application program interface (API). The consumer can utilize the application to store and analyse data without having to worry about managing the infrastructure, service, or software, as that falls to the CSP.

- **FaaS (Function as a Service)** is a cloud computing service that allows the consumer to develop, manage, and run their application functionalities without having to manage and maintain any of the infrastructure that is required. The consumer can execute code in response to events that happen within the CSP or the application without having to build out or maintain a complex underlying infrastructure.

To complicate things even more, a cloud environment has multiple deployment models:

- **Private cloud (on-prem)** consists of all the computing resources being hosted and used exclusively in private tenancy by one consumer (enterprise) within its own offices and data centres. The consumer is responsible for the operational costs, hardware, software, and the resources required to build and maintain the infrastructure. This is best used for critical business operations that want to control all access, including physical access, to the cloud system.

- **Private cloud (third-party hosted)** is a private tenancy cloud system that is hosted by an external third-party provider. The third-party provides an exclusive use cloud environment for the consumer to deploy applications and store data on. The third-party provides the hardware, software, servers, supporting infrastructure and sometimes staff, which offers the customer a reduced, up front capital investment and access to additional resources as needed. This model can be useful for enterprises that have elastic computing needs; have specific regulatory requirements that can be met at scale by a third-party much cheaper than on-prem; or for enterprises that do not wish to make a large capital investment in IT infrastructure and would rather pay as they go.

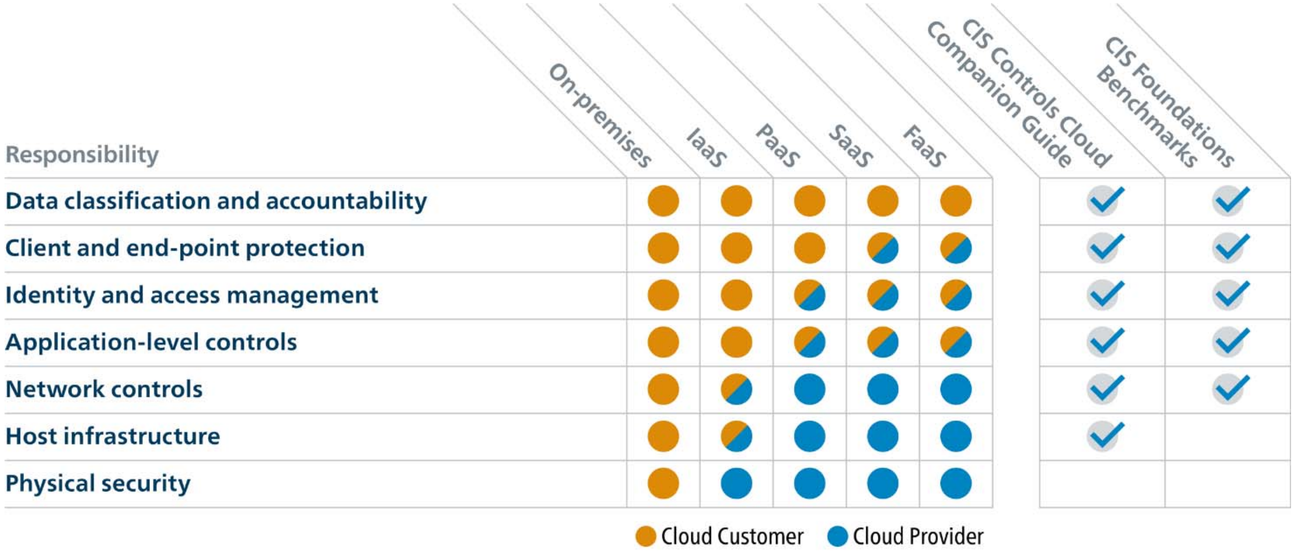
- **Community cloud (shared)** is a deployment solution where the computing resources and infrastructure are shared between several enterprises or community of consumers. The resources can be managed internally or by a third-party and they can be hosted on-prem or externally. The enterprises share the cost and often have similar cloud security requirements and business objectives.

- **Public cloud** is an infrastructure and computing service hosted by a third-party company defined as a CSP and exists on the CSP's premises. It is available over the internet and the services can be delivered through a self-service portal. Public cloud is provisioned for open use by the general public and the consumer is provided on-demand access and scalability without the higher overhead cost of maintaining a private cloud environment, but gives up private tenancy. The CSP is responsible for the management and maintenance of the system while the consumer pays only for resources they use. This type of cloud system depends on a "*shared security responsibility model*".

- **Hybrid cloud** is an environment that uses a combination of the two or more cloud deployment models, private cloud (on-prem), private cloud (third-party hosted), and public cloud with an orchestration service between the unique deployment models. A hybrid cloud system can provide more flexibility than exclusively utilizing a public, private, or community cloud system.

Shared Responsibility Model

In the public cloud, there's a shared responsibility between the Cloud Service Provider (CSP) and the user. Security for things like data classification, network controls, and physical security need clear owners. The division of these responsibilities is known as the shared responsibility model for cloud security. Figure 4.1-1 portrays how the responsibilities are shared within different cloud environments.



Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks
Data classification and accountability	🟠	🟠	🟠	🟠	🟠	✓	✓
Client and end-point protection	🟠	🟠	🟠	◐	◐	✓	✓
Identity and access management	🟠	🟠	◐	◐	◐	✓	✓
Application-level controls	🟠	🟠	◐	◐	◐	✓	✓
Network controls	🟠	◐	🔵	🔵	🔵	✓	✓
Host infrastructure	🟠	◐	🔵	🔵	🔵	✓	
Physical security	🟠	🔵	🔵	🔵	🔵		

🟠 Cloud Customer 🔵 Cloud Provider

Figure 4.1-1

Responsibilities under the model will vary depending on the cloud environment within which the user is operating. Irrespective of the cloud service used (IaaS, PaaS, SaaS, or FaaS), protection of the user organization data is that of the organization. Additional guidance for implementing a shared responsibility model is available [i.30].

Methodology

A consistent approach is needed for analysing the Controls in the context for cloud. For each of the Controls, the following information is provided:

- **Cloud Applicability** - The applicability field assesses the degree to which a Control functions within the cloud space and which service model should be considered.
- **Cloud Service and Deployment Considerations** - Service and deployment model considerations further define who is responsible for the Controls within the service model it is applicable to and what the consumer of the CSP is responsible for.
- **Cloud Additional** - This is a general area for any additional guidance that also needs to be noted. For instance, relevant tools, products, or threat information that could be of use can be found here.

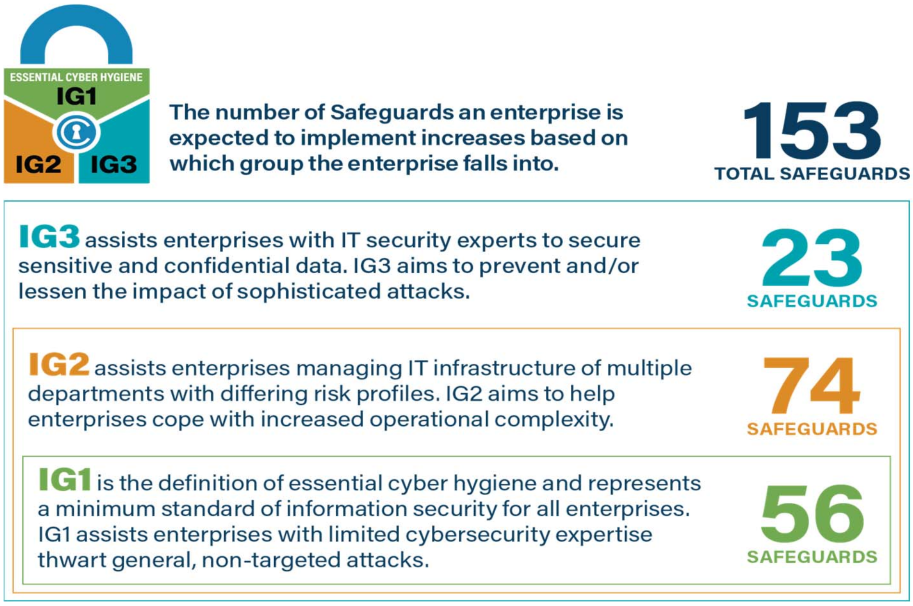
Document Use

The present document provides guidance on how to apply the security best practices found in the latest Critical Security Controls. ETSI TR 103 305-1 [i.20] to any cloud environment from the consumer/customer perspective. For each top-level Control, there is a brief discussion on how to interpret and apply it in such environments, along with any unique considerations or differences from common IT environments.

The applicability of specific Controls and Safeguards is addressed, and additional steps needed in any cloud environment are explained, based on the individual service models. Throughout the present document, the unique mission/business requirements found in cloud environments are taken into consideration, as well as the unique risks (vulnerabilities, threats, consequences, and security responsibilities), which in turn drive the priority of the security requirements (e.g. availability, integrity and confidentiality of process data).

This Technical Report provides guidance to tailor the Controls in the context of a specific IT/Operational Technology (OT) cloud enterprise as an essential starting point for a security improvement assessment and roadmap. OT is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. The present document is also aimed at guiding enterprises involved in the agile software development process via utilization of cloud-based services. DevSecOps, which is short for development, security, and operations, automates the integration of security at every phase of the software and its underlying infrastructure development lifecycle, from initial design through integration, testing, deployment, and software delivery. Control 16 will cover these aspects.

As part of the latest Critical Security Controls [i.20], the Implementation Groups (IGs) are a guideline to help enterprises determine a starting point for implementation of the Controls. Enterprises will, at times, find the need to implement Safeguards in a higher IG. When integrating new technology into an environment, such as cloud, an enterprise should fully consider, and assess the security risks and impacts to assets and data. That understanding should drive the selection and implementation of appropriate Safeguards regardless of IG. Small and Medium size Entities (SME) are included in IG1.



The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

153 TOTAL SAFEGUARDS

IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 SAFEGUARDS

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 SAFEGUARDS

IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 SAFEGUARDS

Figure 4.1-2

4.2 Applicability Overview

Table 4.2-1

Applicability of Service Model					
Control	**Safeguard Title**	**IaaS**	**PaaS**	**SaaS**	**FaaS**
1	Inventory and Control of Enterprise Assets	■	■		
2	Inventory and Control of Software Assets	■	■	■	■
3	Data Protection	■	■	▒	▒
4	Secure Configuration of Enterprise Assets and Software	■	■	▒	▒
5	Account Management	■	■	■	■
6	Access Control Management	■	■	■	■
7	Continuous Vulnerability Management	■	■	▒	▒
8	Audit Log Management	■	■	■	■
9	Email and Web Browser Protections	■	■	■	▒
10	Malware Defences	■	■		
11	Data Recovery	■	■	■	■
12	Network Infrastructure Management	■	▒	▒	▒
13	Network Monitoring and Defence	■	▒	▒	▒
14	Security Awareness and Skills Training	■	■	■	■
15	Service Provider Management	■	■	■	■
16	Application Software Security	■	■	■	■
17	Incident Response Management	■	■	■	■
18	Penetration Testing	■	■	■	■
Applicability Overview for each Service Model:					
■	More than 60 % of Control Safeguards Apply				
▒	Between 60 % and 0% of the Control Safeguards Apply				
	0 %				

4.3 Applying the Critical Security Controls and Safeguards

4.3.1 CONTROL 01 Inventory and Control of Enterprise Assets

Cloud Applicability. The first Control is considered the most important because it is necessary to first identify the systems and devices, including virtual implementations, that need to be secured. Control 1 is about taking inventory. Understanding and solving the asset inventory and device visibility problem is critical in managing a business security program. This is challenging in cloud environments due to the shared security responsibility and the cloud service model utilized.

Table 4.3.1-1

Control 1: Inventory and Control of Enterprise Assets				Implementation Groups			Applicability of Service Model			
Safeguard	**Asset Type**	**Security Function**	**Safeguard Title (See [i.20] for description)**	**IG1**	**IG2**	**IG3**	**IaaS**	**PaaS**	**SaaS**	**FaaS**
1.1	Devices	Identity	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●	●	●		
1.2	Devices	Respond	Address Unauthorized Assets	●	●	●	●	●		
1.3	Devices	Detect	Utilize an Active Discovery Tool		●	●	●	●		
1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●	●	●		
1.5	Devices	Detect	Use a Passive Asset Discovery Tool			●	●	●		

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or its community are using. See clause 4.1.

Cloud Service and Deployment Considerations

- **On-prem** - The local administrator (cloud consumer) is responsible for the security of everything (physical and virtual servers, room, network, as well as storage, hypervisor, operating systems, etc.).
- **IaaS** - The administrator (cloud consumer) deploys, operates, and maintains the virtual networks and virtual machines within this service model but does not manage the underlying cloud infrastructure (physical servers, physical network, physical storage, hypervisor, etc.) as that is the responsibility of the CSP.
- **PaaS** - The administrator (cloud consumer) manages the development, testing, and deployment of their applications. They have full control over the applications and in some cases the host environment settings and operating systems. The CSP is responsible for the physical servers, physical network, storage, hypervisor, and operating systems. The shared responsibility model may apply per clause 4.1. DHCP logging, port level access control might not be applicable.
- **SaaS** - This is not applicable for the cloud consumer as SaaS and FaaS are under software assets. The CSP is responsible for everything but the data.
- **FaaS** - This is not applicable for the cloud consumer as SaaS and FaaS are under software assets. The CSP is responsible for everything but the data.

Cloud Additional Considerations

- In a cloud environment, assets in on-prem, IaaS, or PaaS service models are virtual and can be in the form of virtual machines, virtual networks, virtual switches, etc. with limited exceptions such as dedicated Hardware Security Models (HSMs).
- Due to the nature of virtual systems and the ease to bring online a new virtual asset, it is imperative to maintain a comprehensive list of all the cloud hardware and virtual assets managed.
- It is always up to the consumer to request documentation outlining how the CSP is securing the infrastructure and technology that falls under their responsibility.
- When collecting asset inventory, include the criticality of the asset, the operating system and version, when the asset was discovered, and the asset tag if applicable.
- If containers are considered as FaaS, then the CSP is often not responsible for maintaining security of the containers or the microservices that run within. Under this circumstance, containers should be treated under Control 2, below.

4.3.2 CONTROL 02 Inventory and Control of Software Assets

Cloud Applicability. The second Control offers the guidance needed to identify, track, and account for all software utilized in an environment. This is challenging in cloud environments due to the shared security responsibility and the cloud service model utilized.

Table 4.3.2-1

Control 2: Inventory and Control of Software Assets				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
2.1	Applications	Identify	Establish and Maintain a Software Inventory	●	●	●	●	●	●	●
2.2	Applications	Identify	Ensure Authorized Software is Currently Supported	●	●	●	●	●	●	
2.3	Applications	Respond	Address Unauthorized Software	●	●	●	●	●	●	●
2.4	Applications	Detect	Utilize Automated Software Inventory Tools		●	●	●	●	●	
2.5	Applications	Protect	Allowlist Authorized Software		●	●	●	●		
2.6	Applications	Protect	Allowlist Authorized Libraries		●	●	●	●		
2.7	Applications	Protect	Allowlist Authorized Scripts			●	●	●		●

When considering deployment models, these CSC Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, implement the service/deployment model(s) the enterprise or community are using. See also, Shared Responsibility Model, clause 4.1.

Cloud Service and Deployment Considerations

- **On-prem** - The local administrator is responsible for keeping the inventory of all software utilized regardless of the service model.
- **IaaS** - The administrator (cloud consumer) deploys, operates, and maintains the software utilized within this service model but does not manage the underlying cloud software such as the hypervisor, host operating system, or applications that provide specific services that are the responsibility of the CSP.
- **PaaS** - The administrator (cloud consumer) manages the development, testing, and deployment of their software and applications. They have full control over the applications and in some cases the operating systems so they are responsible for all software running at this level per the Shared Responsibility Model, clause 4.1 . The CSP is responsible for the hypervisor and operating systems and other applications that provide this service. Application whitelisting, whitelisting of libraries, whitelisting of scripts, and segregating high-risk applications will not be applicable to all PaaS service models.
- **SaaS** - The administrator (cloud consumer) is responsible for registering the software on the inventory list as approved. They are also responsible for checking that the vendor still supports and issues updates for the software, and for keeping a record of this in the software inventory. Tracking software inventory could be manual.
- **FaaS** - The administrator (cloud consumer) is responsible for maintaining an inventory of authorized software. Tracking software inventory could be manual.

Cloud Additional Considerations

- In a cloud environment, running on-prem, IaaS, PaaS, SaaS, or FaaS, the software being used and maintained has to be inventoried, patched, and monitored when applicable.
- It is imperative to maintain a comprehensive list of these cloud software assets to identify and mitigate any vulnerabilities and data associated with the software managed.
- It is always up to the consumer to request documentation from the CSP outlining their responsibilities on how the CSP is securing the infrastructure and technology.
- Also keep in mind that as part of the software inventory, the consumer should include the API endpoints.

NOTE: For PaaS using managed Kubernetes® services - which is a logical abstraction for a deployed group of pods in a cluster which all perform the same function - the cloud consumer is responsible for patches/updates.

- Discovery and inventory capabilities should extend to software running inside containers (in the case of Containers-as-a-Service). CaaS is considered a subset of IaaS and is found between IaaS and PaaS.

4.3.3 CONTROL 03 Data Protection

Cloud Applicability. The focus of this Control is on data protection and ensuring the privacy and integrity of sensitive information. The cloud environment is not an exception to private data. If cloud consumers have realized anything while migrating information to the cloud, it is that protecting data can be more complicated. It is a growing concern for CSPs and consumers because any data leakage can go undetected for long periods of time.

Table 4.3.3-1

Control 3: Data Protection				Implementation Groups			Applicability of Service Model			
Safeguard	**Asset Type**	**Security Function**	**Safeguard Title (See [i.20] for description)**	**IG1**	**IG2**	**IG3**	**IaaS**	**PaaS**	**SaaS**	**FaaS**
3.1	Data	Identify	Establish and Maintain a Data Management Process	●	●	●	●	●	●	●
3.2	Data	Identify	Establish and Maintain a Data Inventory	●	●	●	●	●	●	●
3.3	Data	Protect	Configure Data Access Control Lists	●	●	●	●	●	●	●
3.4	Data	Protect	Enforce Data Retention	●	●	●	●	●	●	●
3.5	Data	Protect	Securely Dispose of Data	●	●	●	●	●	●	●
3.6	Devices	Protect	Encrypt Data on End-User Devices	●	●	●				
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme		●	●	●	●	●	●
3.8	Data	Identify	Document Data Flows		●	●	●	●	●	●
3.9	Data	Protect	Encrypt Data on Removable Media		●	●				
3.10	Data	Protect	Encrypt Sensitive Data in Transit		●	●	●	●	●	●
3.11	Data	Protect	Encrypt Sensitive Data At Rest		●	●	●	●		
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity		●	●	●			
3.13	Data	Protect	Deploy a Data Loss Prevention Solution			●	●			
3.14	Data	Detect	Log Sensitive Data Access			●	●	●	●	●

Cloud Service and Deployment Considerations

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, need to defer to the service/deployment model(s) the enterprise or community are using:

- **Private (on-prem)** - The administrator (cloud consumer) is responsible for all of the data regardless of the service model used.

- **IaaS** - The administrator (cloud consumer) is responsible for data protection but is limited to the virtual networks and virtual machines within this service model. The CSP is not responsible for any data loss due to lack of action or security defined for the consumer.

- **PaaS** - The administrator (cloud consumer) manages the data and access for the applications and in some cases the host environment settings and operating systems.

- **SaaS** - The administrator (cloud consumer) is responsible for the data. The CSP is only responsible for making sure the data is online and that access is not granted outside of the application controlled by the cloud consumer.

- **FaaS** - The administrator (cloud consumer) is responsible for the code and any data. The CSP is only responsible for making sure the data is online and that access is not granted outside of the functions called and controlled by the cloud consumer.

Cloud Additional Considerations

- Make sure that the data is not accessible to the public. Encrypt or use tokenisation to protect sensitive data. Encryption has a number of limitations in SaaS solutions and does not allow the data to be searched; however, tokenisation addresses that concern and limitation.

- Control the systems and users that have access to the cloud platform and the data that might be exposed. When hosting any data in the cloud, consider the possible legal implications based on the data classification. More often than not, data protection, redundancy, and backup are the responsibility of the cloud consumer and not the CSP. These shifted responsibilities may alter the applicability of Safeguards 3.11 and 3.13.

4.3.4 CONTROL 04 Secure Configuration of Enterprise Assets and Software

Cloud Applicability. This Control provides guidance for securing hardware and software. As delivered by the CSP, the default configurations for operating systems and applications are normally geared toward ease-of-deployment and ease-of-use - not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software - all can be exploitable in their default state. Even if a strong initial configuration is developed and deployed in the cloud, it should be continually managed to avoid configuration drift as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation of new software or to support new operational requirements. If not, attackers will find opportunities to exploit both network-accessible services and client software.

Table 4.3.4-1

Control 4: Secure Configuration of Enterprise Assets and Software				Implementation Groups			Applicability of Service Model			
Safeguard	**Asset Type**	**Security Function**	**Safeguard Title (See [i.20] for description)**	**IG1**	**IG2**	**IG3**	**IaaS**	**PaaS**	**SaaS**	**FaaS**
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	●	●	●	●	●	●	●
4.2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	●	●	●	●	●		
4.3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets	●	●	●	●	●I		
4.4	Devices	Protect	Implement and Manage a Firewall on Servers	●	●	●	●	●		
4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	●	●	●	●	●		
4.6	Network	Protect	Securely Manage Enterprise Assets and Software	●	●	●	●	●	●	●
4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	●	●	●	●	●	●	●
4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Applications	●	●	●	●	●		
4.9	Devices	Protect	Configure Trusted Domain Name System (DNS) Servers on Enterprise Assets		●	●	●	●		
4.10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices		●	●	●	●		
4.11	Devices	Protect	Enforce Remote Wipe Capability on Portable End-User Devices		●	●	●	●		
4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices			●	●	●		

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **On-prem** - The administrator (cloud consumer) is responsible for the use of a security baseline for all physical and virtual systems, software, and applications.

- **IaaS** - The administrator (cloud consumer) is responsible for utilizing a security baseline for the software, virtual servers, virtual networking, middleware, and applications in the cloud environment.

- **PaaS** - The administrator (cloud consumer) is responsible for utilizing a security baseline for the applications and development tools utilized.

- **SaaS** - The administrator (cloud consumer) is responsible for a security baseline within the software and the data that is being utilized.

- **FaaS** - The administrator (cloud consumer) is responsible for a security baseline within the code and the data being utilized.

Cloud Additional Considerations

- When configuration management tools are used, they should be set to alert-only without automated configuration re-deployment unless it is known to be safe to do so.
- The CSP hosts typical image storage in cloud environments for PaaS, SaaS, and FaaS; therefore, the secure configuration of the underlying servers is the responsibility of the CSP.
- As part of the established secure configurations, SaaS and FaaS should always communicate over TLS and validate the TLS API endpoint certificate.
- Also consider Cloud Access Security Broker (CASB) services that can provide granular controls for monitoring user's application sessions and blocking actions.

4.3.5 CONTROL 05 Account Management

Cloud Applicability. This Control focuses on managing the life cycle of system, application, and user accounts. As part of this management, rules and processes should be established for the creation, use, dormancy, and deletion of all cloud accounts, in order to minimize opportunities for attackers to leverage them. When an employee leaves the enterprise or changes roles, vulnerabilities can arise if employee accounts are not closed or modified. If administrator privileges are loosely and widely distributed, or identical passwords are used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

Table 4.3.5-1

Control 5: Secure Configuration of Enterprise Assets and Software				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	●	●	●	●	●	●	●
5.2	Users	Protect	Use Unique Passwords	●	●	●	●	●	●	●
5.3	Users	Respond	Disable Dormant Accounts	●	●	●	●	●	●	●
5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	●	●	●	●	●	●	●
5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts		●	●	●	●	●	●
5.6	Users	Protect	Centralize Account Management		●	●	●	●	●	●

This Control and Safeguards are applicable to all service and deployment models. For Private (third-party hosted), Public, and Hybrid deployment models, the service/deployment model(s) of the enterprise or community should be used.

Cloud Service and Deployment Considerations

- **Private (on prem)** - The administrator (cloud consumer) is responsible for all accounts regardless of the service model used.
- **IaaS** - The administrator (cloud consumer) is responsible for all accounts utilized on the virtual networks, virtual machines, applications, etc. The CSP is not responsible for this access at the cloud consumer account level.
- **PaaS** - The administrator (cloud consumer) manages the accounts for the applications and in some cases the host operating systems.
- **SaaS** - The administrator (cloud consumer) is responsible for the application accounts.

- **FaaS** - The administrator (cloud consumer) is responsible for the accounts that have the ability to build the code execution based on the cloud functions.

Cloud Additional Considerations

- For consumers operating in the cloud, it is even more important to understand account management. The consumer is responsible for all the accounts.

- The account principle of least privilege access should be followed.

4.3.6 CONTROL 06 Access Management Control

Cloud Applicability. This Control addresses the need for limiting and managing access. The misuse of administrative privileges is a primary method for attackers to spread laterally inside a target enterprise. One of the two primary ways for attackers to spread inside a system is by tricking a user with elevated credentials into opening an email attachment, downloading and running an infected file, and visiting a malicious website from an asset connected to the cloud environment. The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine.

Table 4.3.6-1

Control 6: Access Management Control				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
6.1	Users	Protect	Establish an Access Granting Process	●	●	●	●	●	●	●
6.2	Users	Protect	Establish an Access Revoking Process	●	●	●	●	●	●	●
6.3	Users	Protect	Require MFA for Externally-Exposed Applications	●	●	●	●	●	●	●
6.4	Users	Protect	Require MFA for Remote Network Access	●	●	●	●			
6.5	Users	Protect	Require MFA for Administrative Access	●	●	●	●	●	●	●
6.6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems		●	●	●	●	●	●
6.7	Data	Protect	Centralize Access Control		●	●	●	●	●	●
6.8	Data	Protect	Define and Maintain Role-Based Access Control			●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **Private (on prem)** - The administrator (cloud consumer) is responsible for all accounts regardless of the service model used.

- **IaaS** - The administrator (cloud consumer) is responsible for all accounts utilized on the virtual networks, virtual machines, applications, etc. The CSP is not responsible for this access at the cloud consumer account level.

- **PaaS** - The administrator (cloud consumer) manages the accounts for the applications and in some cases the host operating systems. However, the implementation of a Shared Responsibility Model may alter these management arrangements. See clause 4.1.

- **SaaS** - The administrator (cloud consumer) is responsible for the application accounts.

- **FaaS** - The administrator (cloud consumer) is responsible for the accounts that have the ability to build the code execution based on the cloud functions.

Cloud Additional Considerations

- For consumers operating in the cloud, it is even more important to understand and maintain account control. The consumer is responsible for all the accounts and what level of access those accounts have to their cloud environment.
- When possible, MFA should be required.
- The use of shared service accounts should be limited.
- Permissions should be granted through group membership, as that is easier to manage.
- Role-Based Access Control (RBAC) has become the primary methodology and is a critical capability for managing access to cloud-based resources.
- Apply multi-factor authentication, which will help maintain accountability and configuration

4.3.7 CONTROL 07 Continuous Vulnerability Management

Cloud Applicability. This Control addresses the need for continuous vulnerability management, which can be a significant task in most enterprises. Understanding and managing vulnerabilities in a cloud environment can be more challenging than in traditional IT systems. A cloud environment is dynamic, allowing scaling of the environment at an ever-changing pace. With the increasing use of DevSecOps, the internal landscape is ever-changing. As enterprises migrate to the cloud, they are in a difficult position because of the risks and vulnerabilities associated with the use of cloud services. Giving control of some assets to a third-party depending on the deployment model utilized, and verifying the security and vulnerability status of those assets, is not always the responsibility of cloud consumers. Cloud environments also host cloud-specific vulnerabilities that have to be monitored and managed.

Table 4.3.7-1

Control 7: Continuous Vulnerability Management				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
7.1	Applications	Protect	Establish and Maintain a Vulnerability Management Process	●	●	●	●	●	●	●
7.2	Applications	Respond	Establish and Maintain a Remediation Process	●	●	●	●	●	●	●
7.3	Applications	Protect	Perform Automated Operating System Patch Management	●	●	●	●	●		
7.4	Applications	Protect	Perform Automated Application Patch Management	●	●	●	●	●		●
7.5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets		●	●	●	●		
7.6	Applications	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		●	●	●	●		
7.7	Applications	Respond	Remediate Detected Vulnerabilities		●	●	●	●		

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **On-prem** - The administrator (cloud consumer) is responsible for continuous vulnerability management of the hardware and software, both physical and virtual servers, networking, middleware, and applications utilized.
- **IaaS** - The administrator (cloud consumer) is responsible for continuous vulnerability management of the software, virtual servers, virtual networking, middleware, and applications utilized. The CSP is responsible for continuous vulnerability management with the infrastructure and technology that they provide.

- **PaaS** - The administrator (cloud consumer) is responsible for continuous vulnerability management of the applications and development tools utilized. The CSP is responsible for continuous vulnerability management of the hardware infrastructure and software technology that they provide.

- **SaaS** - Except for Safeguards 7.1 and 7.2, the Safeguards are not applicable for the cloud consumer. The CSP is responsible for everything but the data, vulnerability management and remediation.

- **FaaS** - Except for Safeguards 7.1 and 7.2, the Safeguards are not applicable for the cloud consumer. The CSP is responsible for everything but the code and the data utilized within the functions plus vulnerability management and remediation.

Cloud Additional Considerations

- It is always the cloud consumer's responsibility to request documentation from the CSP detailing how the CSP is securing the infrastructure and the technology they are responsible for.

- The consumer should continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

- When considering PaaS environments, some will have images or stem cells which, by default, do not allow for interactive users such as scanner accounts. The consumer should consider a solution that identifies vulnerabilities without introducing new vulnerabilities and which does not require a dedicated scanner account.

- Some agents have download dependencies that may require opening up proxies or firewalls, which can introduce other risk elements that the consumer has to be aware of.

4.3.8 CONTROL 08 Audit Log Management

Cloud Applicability. This Control offers guidance for the maintenance and monitoring of audit logs. Without protected and complete logging records, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. The CSP helps a consumer meet this Control by providing the ability to generate and monitor audit logs.

Table 4.3.8-1

Control 8: Audit Log Management				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	●	●	●	●	●	●	●
8.2	Network	Detect	Collect Audit Logs	●	●	●	●	●	●	●
8.3	Network	Protect	Ensure Adequate Audit Log Storage	●	●	●	●	●	●	●
8.4	Network	Protect	Standardize Time Synchronization		●	●	●			
8.5	Network	Detect	Collect Detailed Audit Logs		●	●	●	●	●	●
8.6	Network	Detect	Collect DNS Query Audit Logs		●	●	●	●		
8.7	Network	Detect	Collect URL Request Audit Logs		●	●	●	●		
8.8	Devices	Detect	Collect Command-Line Audit Logs		●	●	●	●		
8.9	Network	Detect	Centralize Audit Logs		●	●	●	●	●	●
8.10	Network	Protect	Retain Audit Logs		●	●	●	●	●	●
8.11	Network	Detect	Conduct Audit Log Reviews		●	●	●	●	●	●
8.12	Data	Detect	Collect Service Provider Logs			●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **On-prem** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and processing of the audit logs for all systems.

- **IaaS** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and process analysis of the audit logs for the software, virtual servers, virtual networking, middleware, and applications when applicable in the cloud environment.

- **PaaS** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and process analysis of the audit logs for the applications, operating systems, and development tools utilized when applicable in the cloud environment.

- **SaaS** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and process analysis of the audit logs once they are made available by the CSP. Time sources and the ability to enable logging are dependent on the CSP.

- **FaaS** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and process analysis of the audit logs once they are made available by the CSP. Time sources and the ability to enable logging are dependent on the CSP.

Cloud Additional Considerations

- For SaaS and FaaS solutions, it is often required that the CSP provides the required audit logs and allows for the consumer to access, review, and maintain logs based on the Controls as defined.

- In some cases, the service solution might not support the level of logging recommended by this Control and its Safeguards.

- It is the responsibility of cloud consumers to request the logs from the CSP. The consumer might want to consider creating a secure channel to download logs from the CSP.

- Ensure adequate audit log storage is applicable for IaaS as that is typically where storage will occur and make sure enough storage is allotted for logging of all the services.

- Retain audit logs across enterprise assets for a minimum of 90 days or in accordance to the local regulatory demands.

4.3.9 CONTROL 09 Email and Web Browser Protections

Cloud Applicability. This Control focuses on the security of web browsers and email clients, which are very vulnerable attack vectors. Quite often, cloud environments require internet web access. Depending on the cloud model, there might not be a requirement for email clients, and if email is utilized, it is typically only in an outgoing manner. It is common to have alerts and other message systems in place that monitor critical processes and send out reports via email. These emails are typically accessed from business or corporate assets that are on separate networks. Most web-based applications are now operating in the cloud.

Table 4.3.9-1

Control 9: Email and Web Browser Protections				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
9.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	●	●	●	●	●	●	●
9.2	Network	Protect	Use DNS Filtering Services	●	●	●	●	●		
9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters		●	●	●	●		
9.4	Applications	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		●	●	●	●	●	●
9.5	Network	Protect	Implement DMARC		●	●	●	●	●	
9.6	Network	Protect	Block Unnecessary File Types		●	●	●	●	●	
9.7	Network	Protect	Deploy and Maintain Email Server Anti-Malware Protections			●	●	●	●	

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **On-prem** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the email and web browser security.
- **IaaS** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the email and web browser for the software, virtual servers, virtual networking, middleware, and applications when applicable in the cloud environment.
- **PaaS** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the email and web browser capabilities for the applications, operating systems, and development tools utilized when applicable.
- **SaaS** - The administrator (cloud consumer) is responsible for email and web browser security.
- **FaaS** - The administrator (cloud consumer) is responsible for email and web browser security.

Cloud Additional Considerations

- The rest of the Safeguards related to using authorized browsers, scripting filters, and logging are applicable any browser access running off the servers or systems is utilized.
- Since SaaS and possibly FaaS may be using a web browser to interact with the application, the web browser should be up-to-date. Additionally, any third-party extensions such as Java should be updated and the highest possible security policies should be applied according to the enterprise requirements.
- Ensure that no email clients are installed or present on any servers. Where a device or server has the capability to send email-based alerts or reports, make sure that it is limited to outbound only.

4.3.10 CONTROL 10 Malware Defences

Cloud Applicability. This Control addresses the steps needed to ensure a strong defence against malware intrusions. Malicious code is a very real threat to all environments and the cloud is no exception. While proper network segmentation and defence-in-depth strategies help to mitigate this risk by making it difficult for threat actors to deliver malware to their intended locations, malware defence still needs tools and processes in place to thwart and detect incidents.

Table 4.3.10-1

Control 10: Malware Defences				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
10.1	Devices	Protect	Deploy and Maintain Anti-Malware Software	●	●	●	●	●		
10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	●	●	●	●	●		
10.3	Devices	Protect	Disable Autorun and Autoplay for Removable Media	●	●	●	●			
10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media		●	●	●			
10.5	Devices	Protect	Enable Anti-Exploitation Features		●	●	●	●		
10.6	Devices	Protect	Centrally Manage Anti-Malware Software		●	●	●	●		
10.7	Devices	Detect	Use Behaviour-Based Anti-Malware Software		●	●	●	●		

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **On-prem** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the anti-malware software and other security settings for all physical and virtual devices in place to prevent any intrusions.

- **IaaS** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the anti-malware software and other security settings for the software, virtual servers, virtual networking, middleware, and applications when applicable in the cloud environment.

- **PaaS** - The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the anti-malware software and other security settings for the applications, operating systems, and development tools utilized when applicable.

- **SaaS** - This Control and all of it Safeguards are not applicable for the cloud consumer.

- **FaaS** - This Control and all of it Safeguards are not applicable for the cloud consumer.

Cloud Additional Considerations

- In a cloud environment, there are some instances where the virtual devices do not support the required endpoint software, thus making on-device malware monitoring difficult.

- In the instances where malware defence is not the responsibility of the cloud consumer, it then becomes the responsibility of the CSP.

4.3.11 CONTROL 11 Data Recovery

Cloud Applicability. This Control references the need for performing system backups for data recovery capability. Backing up system data to include user data in the cloud environment is important in all four service models. The ability to protect and recover a system or user data in a timely manner is critical to cloud consumers. The challenge is often for the cloud consumer to remember that the protection and integrity of the user and system data can be their responsibility where the only thing the CSP is guaranteeing is the availability of the data.

Table 4.3.11-1

Control 11: Data Recovery				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
11.1	Data	Recover	Establish and Maintain a Data Recovery Process	●	●	●	●	●	●	●
11.2	Data	Recover	Perform Automated Backups	●	●	●	●	●	●	●
11.3	Data	Protect	Protect Recovery Data	●	●	●	●	●	●	●
11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	●	●	●	●	●	●	●
11.5	Data	Recover	Test Data Recovery		●	●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **On-prem** - The administrator (cloud consumer) is responsible for all data recovery capabilities in the environment.

- **IaaS** - The administrator (cloud consumer) is responsible for data recovery capabilities for all software, virtual servers, virtual networking, middleware, and applications, where applicable, in the cloud environment.

- **PaaS** - The administrator (cloud consumer) is responsible for data recovery capabilities for all applications, hosting environment operating systems settings, and developing the tools utilized.

- **SaaS** - The administrator (cloud consumer) is responsible for data recovery capabilities for the application/software that is running as a service in the cloud environment.

- **FaaS** - The administrator (cloud consumer) is responsible for data recovery capabilities for the code and functions that are running as a service in the cloud environment.

Cloud Additional Considerations

- Data can be utilized and affected by all the Service models.

- When referencing system data, be sure to include user data in that context. This inclusion is what makes this Control and the majority of these CSC Safeguards applicable to a SaaS and FaaS service model.

- The cloud consumer is always responsible for "their" data regardless of the service model. It is imperative that they have backup and/or redundancy in place so that there is no loss of data.

4.3.12 CONTROL 12 Network Infrastructure Management

Cloud Applicability. This Control addresses the need to manage the configuration of the network using architecture diagrams along with authentication, authorization, and auditing. The network infrastructure of a cloud environment should require the same rigorous configuration management and change control process as a physical environment. Attack vectors, although virtual, remain the same with unsecure services, poor firewall and network configurations, and default or legacy credentials.

Table 4.3.12-1

Control 12: Network Infrastructure Management				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
12.1	Network	Protect	Ensure Network Infrastructure is Up-to-Date	●	●	●	●			
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		●	●	●	●	●	●
12.3	Network	Protect	Securely Manage Network Infrastructure		●	●	●	●	●	●
12.4	Network	Identify	Establish and Maintain Architecture Diagram(s)		●	●	●	●	●	●
12.5	Network	Protect	Centralize Network Authentication, Authorization and Auditing (AAA)		●	●	●			
12.6	Network	Protect	Use of Secure Network Management and Communication Protocols		●	●	●			
12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		●	●	●			
12.8	Devices	Protect	Establish and Maintain Dedicated Computing Resources For All Administrative Work			●	●			

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using. Safeguards 12.1, 12.2 and 12.3 may fall within the Shared Responsibility Model. See clause 4.1 which assigns the responsibility for the network controls to the CSP.

Cloud Service and Deployment Considerations

- **On-prem** - The local administrator (cloud consumer) is responsible for the secure configuration of all network devices.

- **IaaS** - The administrator (cloud consumer) deploys, operates, and maintains the virtual networks and web application firewalls within this service model but does not manage the underlying cloud infrastructure like the physical servers, physical network, storage, hypervisor, etc., as that is the responsibility of the CSP.

- **PaaS** - The administrator (cloud consumer) generally manages the application, the host environment network settings, and the development tools network settings. The CSP is generally responsible for the physical servers, physical network, storage, hypervisor, and operating systems. However, a Shared Responsibility Model may exist in some jurisdictions. Refer to clause 4.1.

- **SaaS** - This is not applicable for the cloud consumer. The CSP is responsible for all physical and virtual network device configuration.

- **FaaS** - This is not applicable for the cloud consumer. The CSP is responsible for all physical and virtual network device configuration.

Cloud Additional Considerations

- Ensure all virtual firewalls are configured to deny by default.

- Apply multi-factor authentication, which will help maintain accountability and configuration management.

4.3.13 CONTROL 13 Network Monitoring and Defence

Cloud Applicability. This Control focuses on the importance of managing the flow of information between networks of different trust levels. To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defences should be multi-layered, relying on firewalls, proxies, Demilitarized Zone (DMZ) perimeter networks, network-based Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). It is also critical to filter both inbound and outbound traffic. This can be challenging in a cloud environment, as there is not always the ability to set up multiple layers to the same extent as in a physical setup. Therefore, the boundary changes, along with where that defence is set up. Nonetheless, some defence should be set up.

Table 4.3.13-1

Control 13: Network Monitoring and Defence				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
13.1	Network	Detect	Centralize Security Event Alerting		●	●	●	●	●	●
13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution		●	●	●			
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		●	●	●			
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		●	●	●			
13.5	Devices	Protect	Manage Access Control for Remote Assets		●	●	●			
13.6	Network	Detect	Collect Network Traffic Flow Logs		●	●	●			
13.7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution			●	●			
13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution			●	●			
13.9	Devices	Protect	Deploy Port-Level Access Control			●	●			
13.10	Network	Protect	Perform Application Layer Filtering			●	●			
13.11	Network	Detect	Tune Security Event Alerting Thresholds			●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **On-prem** - The administrator (cloud consumer) is responsible for the network boundary monitoring and defence.

- **IaaS** - The administrator (cloud consumer) deploys, operates, and maintains the virtual networks and virtual infrastructure so they are responsible for boundary defence from the cloud perspective. The CSP is responsible for the underlying cloud infrastructure boundary defence for the physical network.
- **PaaS** - The administrator (cloud consumer) might have some network port control options within the application or the host environment settings and operating systems and the development tools utilized to implement Safeguard 13.4.
- **SaaS** - The majority of these Safeguards are not applicable to the cloud consumer. The CSP would be responsible for the boundary defence.
- **FaaS** - This majority of these Safeguards are not applicable to the cloud consumer. The CSP would be responsible for the boundary defence.

Cloud Additional Considerations

- Maintain and enforce a minimum-security standard for all devices remotely logging into the cloud network for on-prem and IaaS.
- Maintain logging of all activities and traffic that pass through the cloud environment when looking at IaaS service models.
- Recognize that not all traffic, ingress or egress, will necessarily pass through one virtual device or network. For this reason, it is crucial to identify all known and potential means for accessing the cloud environment and the virtual systems and networking.
- Implement a zero-trust policy, requiring authentication and trust for internal network communication.

4.3.14 CONTROL 14 Security Awareness and Skills Training

Cloud Applicability. This Control focuses on educating and training the enterprise workforce in a range of security practices that span from "basic to advanced skills" to "security awareness and vigilance". Human error, oversights, and negligence are leading causes of security weakness, and the consequences of untrained or infrequently trained personnel in a cloud environment can have a range of damaging effects. Regardless of the service model or deployment, security awareness and training are the responsibility of the enterprise operating in the cloud.

Table 4.3.14-1

Control 14: Security Awareness and Skills Training				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
14.1		Protect	Establish and Maintain a Security Awareness Program	●	●	●	●	●	●	●
14.2		Protect	Train Workforce Members to Recognize Social Engineering Attacks	●	●	●	●	●	●	●
14.3		Protect	Train Workforce Members on Authentication Best Practices	●	●	●	●	●	●	●
14.4		Protect	Train Workforce on Data Handling Best Practices	●	●	●	●	●	●	●
14.5		Protect	Train Workforce Members on Causes of Unintentional Data Exposure	●	●	●	●	●	●	●
14.6		Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	●	●	●	●	●	●	●
14.7		Protect	Train Workforce on How to Identify and Report if their Enterprise Assets are Missing Security Updates	●	●	●	●	●	●	●
14.8		Protect	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	●	●	●	●	●	●	●
14.9		Protect	Conduct Role-Specific Security Awareness and Skills Training		●	●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

Private Cloud (on-prem) is not a shared security model like public cloud. So the responsibility is strictly on the organization to provide and meet all security standards.

Be aware that Private Cloud deployments are not necessarily more secure than any other deployment method - it requires diligence and attention to:
Breach Exposure

- Physical Security Risk
- Compliance Issues
- Responsiveness, Capacity, Performance and Uptime

Cloud Considerations

The security awareness and training program is solely the cloud consumer's responsibility. Although the CSP should implement their own security training program, this Control and its applicability to the cloud environment is a requirement for the cloud consumer.

4.3.15 CONTROL 15 Service Provider Management

Cloud Applicability. This Control focuses on evaluating and maintaining the many different service providers that can be utilized by an enterprise. Service providers can be classified as internal, external or shared. They can include many different types from: application, cloud, internet, managed, etc. At times, the service provider will handle and hold the enterprise's sensitive data. When working in the cloud, storing and transferring sensitive data is common; and, based on the shared responsibility of the enterprise operating in the cloud, keeping track of this information is critical.

Table 4.3.15-1

Control 15: Service Provider Management				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
15.1		Identify	Establish and Maintain an Inventory of Service Providers	●	●	●	●	●	●	●
15.2		Identify	Establish and Maintain a Service Provider Management Policy		●	●	●	●	●	●
15.3		Identify	Classify Service Providers		●	●	●	●	●	●
15.4		Protect	Ensure Service Provider Contracts Include Security Requirements		●	●	●	●	●	●
15.5		Identify	Assess Service Providers			●	●	●	●	●
15.6	Data	Detect	Monitor Service Providers			●	●	●	●	●
15.7	Data	Protect	Securely Decommission Service Providers			●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

- **Private (on-prem)** - The administrator (cloud consumer) is responsible for all service provider information. Typically, this will encompass application, network, internet, storage, telecommunications etc.
- **IaaS** - The administrator (cloud consumer) is responsible for the cloud service provider information. Application, network, managed, and storage services among others will all fall to the administrator for information gathering if applicable. The CSP will provide the information to the administrator if requested.

- **PaaS** - The administrator (cloud consumer) is responsible for the cloud service provider information. Application, managed and storage services among others will all fall to the administrator for information gathering if applicable. The CSP will provide the information to the administrator if requested.

- **SaaS** - The administrator (cloud consumer) is responsible for the cloud service provider information and the software service provider if outside of the CSP. Application, network, managed and storage services among others will all fall to the administrator for information gathering if applicable. The CSP will provide the information to the administrator if requested.

- **FaaS** - The administrator (cloud consumer) is responsible for the cloud service provider information. The CSP will provide the information to the Administrator if requested.

Cloud Additional Considerations

- The key to gathering the information required for the service provider Control and the Safeguards is to understand the cloud service provider will fall into all the cloud service models. However, other service providers might be categorized into some of the service models depending on what is being utilized. Therefore, additional information gathering will be required outside of just documenting the CSP.

4.3.16 CONTROL 16 Application Software Security

Cloud Applicability. This Control focuses on the security of applications (in-house developed or acquired off the shelf or from external developers). This is a complex activity requiring a complete program encompassing enterprise-wide policy, technology, and the role of people. Any cloud environment service model or deployment model should be a part of this program. All software should be regularly tested for vulnerabilities when applicable. The operational practice of scanning for application vulnerabilities is consolidated within Control 3: Continuous Vulnerability Management. However, the most effective approach is to implement a full supply chain security program for externally acquired software and a Secure Software Development Life Cycle for internally developed software.

Table 4.3.16-1

Control 16: Application Software Security				Implementation Groups			Applicability of Service Model			
Safeguard	**Asset Type**	**Security Function**	**Safeguard Title (See [i.20] for description)**	**IG1**	**IG2**	**IG3**	**IaaS**	**PaaS**	**SaaS**	**FaaS**
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process		●	●	●	●	●	●
16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		●	●	●	●	●	●
16.3	Applications	Protect	Perform Root Cause Analysis on Security Vulnerabilities		●	●	●	●	●	●
16.4	Applications	Protect	Establish and Manage an Inventory of Third-Party Software Components		●	●	●	●	●	
16.5	Applications	Protect	Use Up-to-Date and Trusted Third-Party Software Components		●	●	●	●	●	
16.6	Applications	Protect	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		●	●	●	●	●	●
16.7	Applications	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure		●	●	●	●	●	●
16.8	Applications	Protect	Separate Production and Non-Production Systems		●	●	●	●	●	●
16.9	Applications	Protect	Train Developers in Application Security Concepts and Secure Coding		●	●	●	●	●	●
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures		●	●	●	●	●	●
16.11	Applications	Protect	Leverage Vetted Modules or Services for Application Security Components		●	●	●	●	●	●
16.12	Applications	Protect	Implement Code-Level Security Checks			●	●	●	●	●
16.13	Applications	Protect	Conduct Application Penetration Testing			●	●	●	●	
16.14	Applications	Protect	Conduct Threat Modelling			●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using. Although many of the Control 16 Application Software Security Safeguards may not be the responsibility of the consumer in SaaS and some FaaS service models, Some Shared Responsibility Models or contractual provisions may enable the Safeguards to be required.

Cloud Service and Deployment Considerations

- **Private (on-prem)** - The administrator (cloud consumer) is responsible for all application software security regardless of the service model used.
- **IaaS** - The administrator (cloud consumer) is responsible for all application software security. The CSP will provide permission and access for scanning the cloud consumer software.
- **PaaS** - The administrator (cloud consumer) manages the application software security for the applications and in some cases the host environment settings and operating systems. The CSP will provide permission and access for scanning the cloud consumer software.
- **SaaS** - The administrator (cloud consumer) is responsible for the secure configuration and management of the application and in some cases other aspects of application software security. The CSP is responsible for making sure the data is online and for providing access for scanning for vulnerabilities by the cloud consumer. The CSP is also responsible for making sure the data is online and for providing access for scanning for vulnerabilities by the cloud consumer.
- **FaaS** - The administrator (cloud consumer) is responsible for the functional code and in some cases other aspects of application software security.

Cloud Additional Considerations

- Depending on the deployment model, scanning applications for vulnerabilities will sometimes require the cloud consumer to request permission from the CSP. As part of this request, the consumer will often have to provide detailed information to include any IP addresses, timeframe, etc.
- If the consumer is utilizing a SaaS service model, the conversation will focus on the CSP's ability to provide the application vulnerability management along with the vulnerability assessment reports for the product if applicable.
- In the SaaS and IaaS service models, there is often the opportunity for vendor-provided API integration. Any vendor-provided APIs or custom-built APIs should be scanned and reviewed.
- Additionally, DevOps teams need to be armed with tools that help them build security in from the start.
- If continuous integration/continuous delivery pipelines are being used, scanning of development artifacts should prevent vulnerable workloads from being released into production and to better build runtime protection profiles.
- Securely manage configuration files for building out the infrastructure the applications run on (Infrastructure as Code - IaC), change management, testing, and deployment for Docker files, Kubernetes® manifests, Helm charts, etc. If utilizing IaC, ensure that secrets are safeguarded that are needed to run applications and systems, as exposed secrets can put the systems at risk.

4.3.17 CONTROL 17 Incident Response Management

Cloud Applicability. This Control focuses on how to manage and respond to a successful cyber-attack against an enterprise. The question of a successful cyber-attack against an enterprise is not "if" but "when". Cyber incidents are now just part of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully manage and recover. Without an incident response plan, an enterprise may not discover an attack in the first place, or, if the attack is detected, the enterprise may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion.

Table 4.3.17-1

Control 17: Incident Response Management				Implementation Groups			Applicability of Service Model			
Safeguard	Asset Type	Security Function	Safeguard Title (See [i.20] for description)	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
17.1		Respond	Designate Personnel to Manage Incident Handling	●	●	●	●	●	●	●
17.2		Respond	Establish and Maintain Contact Information for Reporting Security Incidents	●	●	●	●	●	●	●
17.3		Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	●	●	●	●	●	●	●
17.4		Respond	Establish and Maintain an Incident Response Process		●	●	●	●	●	●
17.5		Respond	Assign Key Roles and Responsibilities		●	●	●	●	●	●
17.6		Respond	Define Mechanisms for Communicating During Incident Response		●	●	●	●	●	●
17.7		Recover	Conduct Routine Incident Response Exercises		●	●	●	●	●	●
17.8		Recover	Conduct Post-Incident Reviews		●	●	●	●	●	●
17.9		Recover	Establish and Maintain Security Incident Thresholds			●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

Incident response and management is no different in the cloud. If process and procedures are in place organisationally, they can be utilized for any of the cloud service and deployment models. The major consideration is where the security management lies and the conversations that with the CSP around the incident.

Cloud Additional Considerations

Throughout the development and documentation of the incident response plan and recovery efforts, the CSP's shared responsibility model should be taken into consideration to identify the areas to be focused upon and those that would primarily fall within customer's realm of responsibility.

4.3.18 CONTROL 18 Penetration Testing

Cloud Applicability. This Control is focused on designing and conducting controlled penetration testing in an operational technology environment, including connected devices and systems regardless of their location and nature (physical, virtual, cloud). Attackers often exploit the gap between good defensive designs and intentions and implementation or maintenance. Examples include: the time window between announcement of a vulnerability, the availability of a vendor patch, and actual installation on every machine. Other examples include: failure to apply good configurations to machines that come on and off of the network; and failure to understand the interaction among multiple defensive tools, or with normal system operations that have security implications.

Penetration tests can provide significant value, but only when basic defensive measures are already in place, and when these tests are performed as part of a comprehensive, ongoing program of security management, and improvement as outlined in the Controls. Each enterprise should define a clear scope and rules of engagement for penetration testing and Red Team analyses. The scope of such projects should include, at a minimum, systems with the enterprise's highest value information and production processing functionality.

Table 4.3.18-1

Control 18: Penetration Testing				Implementation Groups			Applicability of Service Model			
Safeguard	**Asset Type**	**Security Function**	**Safeguard Title (See [i.20] for description)**	**IG1**	**IG2**	**IG3**	**IaaS**	**PaaS**	**SaaS**	**FaaS**
18.1		Identify	Establish and Maintain a Penetration Testing Program		●	●	●	●	●	●
18.2	Network	Identify	Perform Periodic External Penetration Tests		●	●	●	●	●	●
18.3	Network	Protect	Remediate Penetration Test Findings		●	●	●	●	●	●
18.4	Network	Protect	Validate Security Measures			●	●	●	●	●
18.5		Identify	Perform Periodic Internal Penetration Tests			●	●	●	●	●

When considering deployment models, this Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, defer to the service/deployment model(s) the enterprise or community are using.

Cloud Service and Deployment Considerations

Pen testing is no different in the cloud. If related process and procedures in place organisationally exist, they can be utilized for any of the cloud service and deployment models. The major consideration is where the security management lies and the conversations that with the CSP if an exception is detected.

Cloud Considerations

- Running pen tests will require the cloud consumer to request permission from the CSP. As part of this request, the consumer will often have to provide detailed information to include any IPs to be scanned, source IPs, timeframe, etc. A penetration tester might have to obtain credentials to any third-party tools that complement the cloud provider tools available in the security centre to obtain a complete picture of the client's security operations. The penetration tester, when doing a cloud review, will also need, at minimum, the Reader and SecurityReader roles to include access to the cloud provider's security centre.

- While permission to test from the FaaS service provider may be needed, regular testing against the application interface should be a part of this process. Penetration testing against FaaS may require commentary to permit exceptions where this is not practical, or is explicitly prohibited by the FaaS service provider. In the case that pen testing is not practical or is prohibited, source code review should be done in addition to performing security related unit testing.

5 CSA Security Controls

5.1 Cloud Controls Matrix

The CSA Cloud Controls Matrix (CCM) [i.24] is a cybersecurity control framework for cloud computing composed of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology. Version 4 was released in December 2021. It can be used as a tool for the systematic assessment of a cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain. The controls framework is aligned to the CSA Security Guidance for Cloud Computing and is considered a de-facto standard for cloud security assurance and compliance and used for Security, Trust, Assurance and Risk (STAR) attestation and certifications. The CCM includes the following:

- CCM v4 Controls.

- Mappings to multiple other control frameworks.

- Cloud security questionnaire v4.

- Implementation guidelines.

- Auditing guidelines.

- Security metrics.
- Machine readable expressions in JSON, YAML, and OSCAL.

The CCM framework and associated support materials are freely available [i.24].

5.2 Critical Security Controls Mapping to CSA Cloud Controls Matrix

Mappings from the latest version of the Critical Security Controls to the CSA Cloud Controls Matrix is freely available [i.29].

6 EU Cloud Security (EUCS) Scheme

6.1 EUCS Scheme

The EU is creating its own Cloud Security Controls Framework known as the European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) [i.27] to support the EU Cybersecurity Act, EUCSA. [i.4] Critical Security Control mappings to the EUCS controls framework are not provided in the present document.

7 Cloud Data Centre Critical Security Control Hardened Image implementations

7.1 Hardened Virtual Images

Increasingly, more organizations are moving to the cloud data centre implementations, taking advantage of greater flexibility and scalability in ever-changing computing workloads. However, cloud computing presents its own challenges - including how to ensure that virtual machine images are secure. A virtual machine image is a snapshot of a virtual machine used to create a running instance in a virtual environment, and provides the same functionality as a physical computer. Virtual images reside in the cloud and enable cost-effective performance of routine computing operations without investing in local hardware and software.

In a public cloud instantiation, the security of systems and data becomes critical. Hardening limits potential weaknesses that make systems vulnerable to cyber attacks. More secure than a standard image, hardened virtual machine images help protect against denial of service, Unauthorized data access, and other cyber threats. Hardened Images of the Critical Security Controls are configured according to Benchmark recommendations developed through consensus by a global community of cybersecurity experts. Some Hardened Images are also configured to meet specific mandated security requirements.

7.2 Hardened Virtual Images

The array of hardened virtual images for major cloud data centre platforms and different operating systems is constantly evolving [i.28].

Annex A:
Bibliography

- Cross-Border Data Forum (11 July 2023): "Oceans Apart: The EU and US Cybersecurity Certification Standards For Cloud Services".

History

Document history		
V1.1.1	July 2024	Publication