CIS Controls Cloud Companion Guide

Version 8.1

December 2024

CIS Center for Internet Security®

CIS Controls™

Acknowledgements

CIS would like to thank the many security experts who volunteer their time and talent to support the CIS Controls and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors
G. Carpenter, AWS
Randy Mowen, CIS
Robin Regnier, CIS

Contributors
Ginger Anderson, CIS
Tyler Desjardins, Arctic Wolf
Siddiqui Faheem, Al Hilal Bank, United Arab Emirates
Staffan Huslid, Truesec AB
Mosi K. Platt, Security Governance, Risk, Compliance and Assurance Professional
Dr. James Stewart, SME Cybersecurity, The Lynchpin Group
Valecia Stocchetti, CIS

In addition, we want to thank those contributors whose attributions were not available at the time of publication.

Contents

CIS Controls Cloud Applicability

Appendices

Introduction

The CIS Critical Security Controls® (CIS Controls®) are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS 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 CIS Controls come from a wide range of sectors including: retail, manufacturing, healthcare, education, government, defense, and others. While the CIS 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 CIS Controls.

The Center for Internet Security, Inc. (CIS) is a 501(c)(3) nonprofit organization whose mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.

For additional information, go to https://www.cisecurity.org.

We are at a fascinating point in the evolution of what we now call cyber defense. To help us understand the cyber threat, we have seen the emergence of threat information feeds, reports, tools, alert services, standards, and threat-sharing frameworks. To top it all off, we are surrounded by security requirements, risk management frameworks, compliance regimes, regulatory mandates, and so forth. There is no shortage of information available to security practitioners on what they should do to secure their infrastructure. But all of this technology, information, and oversight has become a veritable "Fog of More" — competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings us great benefits, but it also means that our data and applications are distributed across multiple locations, many of which are not within our enterprise's infrastructure.

The CIS Controls started as a grassroots activity to cut through the "Fog of More" and focus on the most fundamental and valuable actions that every enterprise should take. This companion guide will break down and map the applicable Controls and their implementation for the cloud environment. As the CIS Controls continue to be refined and re-worked through the community, the call for CIS Controls guidance for the cloud was identified as one of the high priority companion documents to be developed.

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 your 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 that offers computing resources such as virtual servers, storage, and networking hardware on demand. 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 life cycle while leaving the management of the underlying infrastructure to the CSP.
- **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 analyze 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 centers. 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. When a consumer is using a Community cloud model they do not get to individually define the security and compliance requirements as that is defined by the "community" of companies using those combined resources.
- **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.

These different deployment models led to and now drive the *CIS Controls Cloud Companion Guide.*

Methodology

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

- **Cloud Applicability** | The applicability field assesses the degree to which a CIS 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 Considerations** | 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.

How to Use This Document

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 8.1 to any cloud environment from the consumer/customer perspective. For each top-level CIS Control, there is a brief discussion on how to interpret and apply the CIS Control in such environments, along with any unique considerations or differences from common IT environments.

CIS Controls version 8.1 (v8.1) is an iterative update to version 8.0. As part of our process to evolve the CIS Controls, we establish "design principles" that guide us through any minor or major updates to the document. Our design principles for this revision are context, clarity, and consistency. Context enhances the scope and practical applicability of Safeguards by incorporating specific examples and additional explanations. Clarity aligns with other major security frameworks to the extent practical, while preserving the unique features of the CIS Controls. Consistency maintains continuity for existing CIS Controls users, ensuring little to no change due to this update.

By reading through CIS Controls version 8.1 with this companion guide, the reader should be able to tailor the CIS 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. We should mention that 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. Finally, this 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 life cycle, from initial design through integration, testing, deployment, and software delivery. CIS Control 16 will cover these aspects.

As part of CIS Controls v8.1, the Implementation Groups (IGs) are a guideline to help enterprises determine a starting point for implementation of the CIS Controls. Enterprises will, at times, find the need to implement CIS 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 CIS Safeguards regardless of IG.

	The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.	153 TOTAL SAFEGUARDS
IG3	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	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	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

Applicability Overview for Each Service Model

Applicability of Service Model

- 🟢 More than 60% of CIS Safeguards apply
- ● Between 60% and 0% of the CIS Safeguards apply
- ○ 0%

Control	Control 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 Defenses	🟢	🟢	●	○
11	Data Recovery	🟢	🟢	🟢	🟢
12	Network Infrastructure Management	🟢	●	●	●
13	Network Monitoring and Defense	🟢	●	●	●
14	Security Awareness and Skills Training	🟢	🟢	🟢	🟢
15	Service Provider Management	🟢	🟢	🟢	🟢
16	Application Software Security	🟢	🟢	🟢	🟢
17	Incident Response Management	🟢	🟢	🟢	🟢
18	Penetration Testing	🟢	🟢	🟢	🟢

CIS Controls Cloud Applicability

CONTROL 1

Inventory and Control of Enterprise Assets

Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Cloud Applicability

The first CIS Control is considered the most important because it is necessary to first identify the systems and devices that need to be secured. CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 1.1	Devices	Identify	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain Detailed Enterprise Asset Inventory

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

Safeguard 1.2	Devices	Respond	IG1	IG2	IG3	IaaS	PaaS		

Address Unauthorized Assets

Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 1.3	Devices	Detect		IG2	IG3	IaaS	PaaS		

Utilize an Active Discovery Tool

Utilize an active discovery tool to identify assets connected to the enterprise’s network. Configure the active discovery tool to execute daily, or more frequently.

Safeguard 1.4	Devices	Identify		IG2	IG3				

Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory

Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise’s asset inventory. Review and use logs to update the enterprise’s asset inventory weekly, or more frequently.

Safeguard 1.5	Devices	Detect			IG3				

Use a Passive Asset Discovery Tool

Use a passive discovery tool to identify assets connected to the enterprise’s network. Review and use scans to update the enterprise’s asset inventory at least weekly, or more frequently.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, Community, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (on-prem)** | The local administrator (cloud consumer) is responsible for the security of everything (physical servers, room, network, 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. DHCP logging, port level access control might not be applicable.
- **SaaS** | This is not applicable for the cloud consumer as SaaS and FaaS is 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 is 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 assets you manage.
- 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, you should consider the criticality of the asset, the operating system and version, when the asset was discovered, and the asset tag if applicable.

CONTROL 2

Inventory and Control of Software Assets

Overview

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Cloud Applicability

The second CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 2.1	Software	Identify	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Software Inventory

Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.

Safeguard 2.2	Software	Identify	IG1	IG2	IG3	IaaS	PaaS	SaaS	

Ensure Authorized Software is Currently Supported

Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

Safeguard 2.3	Software	Respond	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Address Unauthorized Software

Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 2.4	Software	Detect	IG1	IG2	IG3	IaaS	PaaS	SaaS	

Utilize Automated Software Inventory Tools

Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

Safeguard 2.5	Software	Protect		IG2	IG3	IaaS	PaaS		

Allowlist Authorized Software

Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

Safeguard 2.6	Software	Protect		IG2	IG3	IaaS	PaaS		

Allowlist Authorized Libraries

Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently

Safeguard 2.7	Software	Protect			IG3	IaaS	PaaS		FaaS

Allowlist Authorized Scripts

Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1 and .py files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, Community, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (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 like the hypervisor, operating systems, or applications that provide specific services as that is 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. 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 that you manage.
- 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.
- For PaaS with managed Kubernetes services, the cloud consumer is responsible for patches/updates on the Worker Notes.
- 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.
- 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.

CONTROL 3

Data Protection

Overview

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Cloud Applicability

The focus of this CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 3.1	Data	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Data Management Process

Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.2	Data	Identify	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Data Inventory

Establish and maintain a data inventory based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

Safeguard 3.3	Data	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Configure Data Access Control Lists

Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 3.4	Data	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Enforce Data Retention

Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.

Safeguard 3.5	Data	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Securely Dispose of Data

Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

Safeguard 3.6	Data	Protect	IG1	IG2	IG3	IaaS	PaaS		

Encrypt Data on End-User Devices

Encrypt data on end-user devices containing sensitive data. Example implementations can include, Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

Safeguard 3.7	Data	Identify		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Data Classification Scheme

Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.8	Data	Identify		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Document Data Flows

Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.9	Data	Protect		IG2	IG3				

Encrypt Data on Removable Media

Encrypt data on removable media.

Safeguard 3.10	Data	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Encrypt Sensitive Data in Transit

Encrypt sensitive data in transit. Example implementations can include, Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 3.11	Data	Protect		IG2	IG3	IaaS	PaaS		

Encrypt Sensitive Data At Rest

Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

Safeguard 3.12	Data	Protect		IG2	IG3	IaaS			

Segment Data Processing and Storage Based on Sensitivity

Segment data processing and storage, based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

Safeguard 3.13	Data	Protect			IG3	IaaS			

Deploy a Data Loss Prevention Solution

Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's data inventory.

Safeguard 3.14	Data	Detect			IG3	IaaS	PaaS	SaaS	FaaS

Log Sensitive Data Access

Log sensitive data access, including modification and disposal.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is 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 tokenization to protect sensitive data. Encryption has a number of limitations in SaaS solutions and does not allow the data to be searched; however, tokenization 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.

CONTROL 4

Secure Configuration of Enterprise Assets and Software

Overview

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Cloud Applicability

This CIS 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 must 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 4.1	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Secure Configuration Process

Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 4.2	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS		

Establish and Maintain a Secure Configuration Process for Network Infrastructure

Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 4.3	Devices	Protect	IG1	IG2	IG3	IaaS	PaaS		

Configure Automatic Session Locking on Enterprise Assets

Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

Safeguard 4.4	Devices	Protect	IG1	IG2	IG3	IaaS	PaaS		

Implement and Manage a Firewall on Servers

Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

Safeguard 4.5	Devices	Protect	IG1	IG2	IG3	IaaS	PaaS		

Implement and Manage a Firewall on End-User Devices

Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Safeguard 4.6	Devices	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Securely Manage Enterprise Assets and Software

Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol (HTTPS). Do not use insecure management protocols, such as Telnet and HTTP, unless operationally essential.

Safeguard 4.7	Devices	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Manage Default Accounts on Enterprise Assets and Software

Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include, disabling default accounts or making them unusable.

Safeguard 4.8	Devices	Protect	IG1	IG2	IG3	IaaS	PaaS		

Uninstall or Disable Unnecessary Services on Enterprise Assets and Applications

Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Safeguard 4.9	Devices	Protect		IG2	IG3	IaaS	PaaS		

Configure Trusted Domain Name System (DNS) Servers on Enterprise Assets

Configure trusted DNS servers on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 4.10	Devices	Protect		IG2	IG3	IaaS	PaaS		

Enforce Automatic Device Lockout on Portable End-User Devices

Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.

Safeguard 4.11	Data	Protect		IG2	IG3	IaaS	PaaS		

Enforce Remote Wipe Capability on Portable End-User Devices

Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Safeguard 4.12	Data	Protect			IG3	IaaS	PaaS		

Separate Enterprise Workspaces on Mobile End-User Devices

Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (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.

CONTROL 5

Account Management

Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Cloud Applicability

This CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 5.1	Users	Identify	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain an Inventory of Accounts

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator, and service accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Safeguard 5.2	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Use Unique Passwords

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 5.3 **Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 5.4 **Restrict Administrator Privileges to Dedicated Administrator Accounts** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged, account.	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 5.5 **Establish and Maintain an Inventory of Service Accounts** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify		IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 5.6 **Centralize Account Management** Centralize account management through a directory or identity service.	Users	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, Community, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **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 and maintain account management. The consumer is responsible for all the accounts.
- The account principle of least privilege access should be followed.

CONTROL 6

Access Control Management

Overview

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Cloud Applicability

This CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 6.1	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish an Access Granting Process

Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 6.2	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish an Access Revoking Process

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 6.3	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Require MFA for Externally-Exposed Applications

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or single sign-on (SSO) provider is a satisfactory implementation of this Safeguard.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 6.4	Users	Protect	IG1	IG2	IG3	IaaS			

Require MFA for Remote Network Access

Require MFA for remote network access.

Safeguard 6.5	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Require MFA for Administrative Access

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

Safeguard 6.6	Software	Identify		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain an Inventory of Authentication and Authorization Systems

Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

Safeguard 6.7	Users	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Centralize Access Control

Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

Safeguard 6.8	Users	Govern			IG3	IaaS	PaaS	SaaS	FaaS

Define and Maintain Role-Based Access Control

Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **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 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. By design PaaS doesn't allow access to the virtual network. In this case MFA Access is limited to the applications as outlined in Safeguard 6.3.
- 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.

CONTROL 7

Continuous Vulnerability Management

Overview

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Cloud Applicability

This CIS 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 you to scale your 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 you are utilizing, 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 7.1	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Vulnerability Management Process

Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 7.2	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Remediation Process

Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 7.3 **Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Software	Protect	IG1	IG2	IG3	IaaS	PaaS		
Safeguard 7.4 **Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Software	Protect	IG1	IG2	IG3	IaaS	PaaS		FaaS
Safeguard 7.5 **Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.	Software	Identify		IG2	IG3	IaaS	PaaS		
Safeguard 7.6 **Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets** Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.	Software	Identify		IG2	IG3	IaaS	PaaS		
Safeguard 7.7 **Remediate Detected Vulnerabilities** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	Software	Respond		IG2	IG3	IaaS	PaaS		

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (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** | The administrator (cloud consumer) is responsible for the vulnerability management process and remediation process. The CSP is responsible for the automated patch management and vulnerability scans.
- **FaaS** | The administrator (cloud consumer) is responsible for the vulnerability management process and remediation process. The CSP is responsible for the automated patch management and vulnerability scans.

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.

CONTROL 8

Audit Log Management

Overview

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Cloud Applicability

This CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 8.1	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain an Audit Log Management Process

Establish and maintain a documented audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 8.2	Data	Detect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Collect Audit Logs

Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 8.3	Data	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	

Ensure Adequate Audit Log Storage

Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 8.4	Data	Protect		IG2	IG3	IaaS			

Standardize Time Synchronization

Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 8.5 **Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	Data	Detect		IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 8.6 **Collect DNS Query Audit Logs** Collect DNS query audit logs on enterprise assets, where appropriate and supported.	Data	Detect		IG2	IG3	IaaS	PaaS		
Safeguard 8.7 **Collect URL Request Audit Logs** Collect URL request audit logs on enterprise assets, where appropriate and supported.	Data	Detect		IG2	IG3	IaaS	PaaS		
Safeguard 8.8 **Collect Command-Line Audit Logs** Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH, and remote administrative terminals.	Data	Detect		IG2	IG3	IaaS	PaaS		
Safeguard 8.9 **Centralize Audit Logs** Centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process. Example implementations include leveraging a SIEM tool to centralize multiple log sources.	Data	Detect		IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 8.10 **Retain Audit Logs** Retain audit logs across enterprise assets for a minimum of 90 days.	Data	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 8.11 **Conduct Audit Log Reviews** Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.	Data	Detect		IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 8.12 **Collect Service Provider Logs** Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events; data creation and disposal events; and user management events.	Data	Detect			IG3	IaaS	PaaS	SaaS	FaaS

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (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 you have to make sure you have allotted enough storage 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.

CONTROL 9

Email and Web Browser Protections

Overview

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Cloud Applicability

This CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 9.1	Software	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

Safeguard 9.2	Devices	Protect	IG1	IG2	IG3	IaaS	PaaS		

Use DNS Filtering Services

Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.

Safeguard 9.3	Network	Protect	IG1	IG2	IG3	IaaS	PaaS		

Maintain and Enforce Network-Based URL Filters

Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 9.4 **Restrict Unnecessary or Unauthorized Browser and Email Client Extensions** Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	Software	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 9.5 **Implement DMARC** To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	Network	Protect		IG2	IG3	IaaS	PaaS	SaaS	
Safeguard 9.6 **Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.	Network	Protect		IG2	IG3	IaaS	PaaS	SaaS	
Safeguard 9.7 **Deploy and Maintain Email Server Anti-Malware Protections** Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Network	Protect			IG3	IaaS	PaaS	SaaS	

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (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 if you utilize any browser access off the servers or systems that you are running.
- 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 your enterprise requirements.
- Ensure that no email clients are installed or present on any servers. Where a device or system has the capability to send email-based alerts or reports, make sure that it is limited to outbound only.

CONTROL 10

Malware Defenses

Overview

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Cloud Applicability

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

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 10.1 **Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	Devices	Detect	IG1	IG2	IG3	IaaS	PaaS		
Safeguard 10.2 **Configure Automatic Anti-Malware Signature Updates** Configure automatic updates for anti-malware signature files on all enterprise assets.	Devices	Protect	IG1	IG2	IG3	IaaS	PaaS		
Safeguard 10.3 **Disable Autorun and Autoplay for Removable Media** Disable autorun and autoplay auto-execute functionality for removable media.	Devices	Protect	IG1	IG2	IG3	IaaS			
Safeguard 10.4 **Configure Automatic Anti-Malware Scanning of Removable Media** Configure anti-malware software to automatically scan removable media.	Devices	Detect		IG2	IG3	IaaS			

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 10.5	Devices	Protect		IG2	IG3	IaaS	PaaS		

Enable Anti-Exploitation Features

Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 10.6	Devices	Protect		IG2	IG3	IaaS	PaaS		

Centrally Manage Anti-Malware Software

Centrally manage anti-malware software.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 10.7	Devices	Detect		IG2	IG3	IaaS	PaaS		

Use Behavior-Based Anti-Malware Software

Use behavior-based anti-malware software.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (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 defense is not the responsibility of the cloud consumer, it then becomes the responsibility of the CSP.

CONTROL 11
Data Recovery

Overview

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Cloud Applicability

This CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 11.1 **Establish and Maintain a Data Recovery Process** Establish and maintain a documented data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 11.2 **Perform Automated Backups** Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	Data	Recover	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS
Safeguard 11.3 **Protect Recovery Data** Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Data	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 11.4	Data	Recover	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain an Isolated Instance of Recovery Data

Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

Safeguard 11.5	Data	Recover		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Test Data Recovery

Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (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 CIS Control 11 and all the Safeguards within this Control 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.

CONTROL 12

Network Infrastructure Management

Overview

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Cloud Applicability

This CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 12.1	Network	Protect	IG1	IG2	IG3	IaaS			

Ensure Network Infrastructure is Up-to-Date

Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

Safeguard 12.2	Network	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Secure Network Architecture

Design and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Example implementations may include documentation, policy, and design components.

Safeguard 12.3	Network	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Securely Manage Network Infrastructure

Securely manage network infrastructure. Example implementations include version-controlled Infrastructure-as-Code (IaC), and the use of secure network protocols, such as SSH and HTTPS.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 12.4	Documentation	Govern		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain Architecture Diagram(s)

Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 12.5	Network	Protect		IG2	IG3	IaaS			

Centralize Network Authentication, Authorization, and Auditing (AAA)

Centralize network AAA.

Safeguard 12.6	Network	Protect		IG2	IG3	IaaS			

Use of Secure Network Management and Communication Protocols

Use secure network management and communication protocols (e.g. 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

Safeguard 12.7	Network	Protect		IG2	IG3	IaaS			

Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure

Require users to authenticate using MFA to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

Safeguard 12.8	Network	Protect			IG3	IaaS			

Establish and Maintain Dedicated Computing Resources For All Administrative Work

Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (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) manages the application, and at time some of the host environment network settings, and the development tools network settings. The CSP is responsible for the physical servers, physical network, storage, hypervisor, and operating systems.
- **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.
- Sometimes SaaS or FaaS has access externally or internally and there is some networking aspects that can be controlled by the consumer. Control usually happens at the IaaS of PaaS level but it should be considered when utilizing the additional service models.

CONTROL 13

Network Monitoring and Defense

Overview

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Cloud Applicability

This CIS 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 defenses 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 you do not always have the ability to set up multiple layers to the same extent you can in a physical setup. Therefore, your boundary changes, along with where you set up that defense. Nonetheless, you still have to set up some defense.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 13.1	Network	Detect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Centralize Security Event Alerting

Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a security information and event management (SIEM), which includes vendor-defined event correlation alerts; a log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

Safeguard 13.2	Devices	Detect		IG2	IG3	IaaS			

Deploy a Host-Based Intrusion Detection Solution

Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Safeguard 13.3	Network	Detect		IG2	IG3	IaaS			

Deploy a Network Intrusion Detection Solution

Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent Cloud Service Provider (CSP) service.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 13.4	Network	Protect		IG2	IG3	IaaS			

Perform Traffic Filtering Between Network Segments

Perform traffic filtering between network segments, where appropriate.

Safeguard 13.5	Devices	Protect		IG2	IG3	IaaS			

Manage Access Control for Remote Assets

Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

Safeguard 13.6	Network	Detect		IG2	IG3	IaaS			

Collect Network Traffic Flow Logs

Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

Safeguard 13.7	Devices	Protect			IG3	IaaS			

Deploy a Host-Based Intrusion Prevention Solution

Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

Safeguard 13.8	Network	Protect			IG3	IaaS			

Deploy a Network Intrusion Prevention Solution

Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

Safeguard 13.9	Network	Protect			IG3	IaaS			

Deploy Port-Level Access Control

Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

Safeguard 13.10	Network	Protect			IG3	IaaS			

Perform Application Layer Filtering

Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

Safeguard 13.11	Network	Detect			IG3	IaaS	PaaS	SaaS	FaaS

Tune Security Event Alerting Thresholds

Tune security event alerting thresholds monthly, or more frequently.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **Private (on-prem)** | The administrator (cloud consumer) is responsible for the network boundary monitoring and defense.
- **IaaS** | The administrator (cloud consumer) deploys, operates, and maintains the virtual networks and virtual infrastructure so they are responsible for boundary defense from the cloud perspective. The CSP is responsible for the underlying cloud infrastructure boundary defense for the physical network.
- **PaaS** | The administrator (cloud consumer) might have some network port control options within the application or the host environment settings, operating systems, and the development tools utilized to apply some deny communications such as block API calls, disable the internet all together, as outlined in Safeguard 13.4.
- **SaaS** | The administrator (cloud consumer) is responsible for the application software access. The CSP is only responsible for security of the application and making sure the data is online and for providing access for scanning for vulnerabilities by the cloud consumer.
- **FaaS** | The majority of these Safeguards are not applicable to the cloud consumer. The CSP would be responsible for the boundary defense.

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 your cloud environment and the virtual systems and networking.
- Implement a zero-trust policy, requiring authentication and trust for internal network communication.

CONTROL 14

Security Awareness and Skills Training

Overview

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Cloud Applicability

This CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 14.1	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Security Awareness Program

Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 14.2	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Train Workforce Members to Recognize Social Engineering Attacks

Train workforce members to recognize social engineering attacks, such as phishing, pretexting, and tailgating.

Safeguard 14.3	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Train Workforce Members on Authentication Best Practices

Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 14.4	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Train Workforce on Data Handling Best Practices

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

Safeguard 14.5	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Train Workforce Members on Causes of Unintentional Data Exposure

Train workforce members to be aware of causes for unintentional data exposure. Example topics include misdelivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

Safeguard 14.6	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Train Workforce Members on Recognizing and Reporting Security Incidents

Train workforce members to be able to recognize a potential incident and be able to report such an incident.

Safeguard 14.7	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Train Workforce on How to Identify and Report if their Enterprise Assets are Missing Security Updates

Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

Safeguard 14.8	Users	Protect	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

Safeguard 14.9	Users	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Conduct Role-Specific Security Awareness and Skills Training

Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

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 CIS Control and its applicability to the cloud environment is a requirement for the cloud consumer.

CONTROL 15

Service Provider Management

Overview

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Cloud Applicability

This CIS 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 your enterprise's sensitive data. When working in the cloud, you are often storing and transferring sensitive data; and, based on the shared responsibility of the enterprise operating in the cloud, keeping track of this information is critical.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 15.1	Users	Identify	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain an Inventory of Service Providers

Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.2	Documentation	Govern		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Service Provider Management Policy

Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.3	Users	Govern		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Classify Service Providers

Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.4	Documentation	Govern		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Ensure Service Provider Contracts Include Security Requirements

Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments, and must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

Safeguard 15.5	Users	Govern			IG3	IaaS	PaaS	SaaS	FaaS

Assess Service Providers

Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organizational Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaire, or other appropriately rigorous process. Reassess service providers annually, at a minimum, or with new and renewed contracts.

Safeguard 15.6	Data	Govern			IG3	IaaS	PaaS	SaaS	FaaS

Monitor Service Providers

Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

Safeguard 15.7	Data	Protect			IG3	IaaS	PaaS	SaaS	FaaS

Securely Decommission Service Providers

Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **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.

CONTROL 16

Application Software Security

Overview

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Cloud Applicability

This CIS 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 CIS 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 16.1	Documentation	Govern		IG2	IG3	IaaS	PaaS		FaaS

Establish and Maintain a Secure Application Development Process

Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 16.2	Documentation	Govern		IG2	IG3	IaaS	PaaS		FaaS

Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 16.3	Software	Protect		IG2	IG3	IaaS	PaaS		FaaS

Perform Root Cause Analysis on Security Vulnerabilities

Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that creates vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

Safeguard 16.4	Software	Identify		IG2	IG3	IaaS	PaaS		

Establish and Manage an Inventory of Third-Party Software Components

Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate the component is still supported.

Safeguard 16.5	Software	Protect		IG2	IG3	IaaS	PaaS		

Use Up-to-Date and Trusted Third-Party Software Components

Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

Safeguard 16.6	Documentation	Govern		IG2	IG3	IaaS	PaaS		FaaS

Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities

Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

Safeguard 16.7	Software	Protect		IG2	IG3	IaaS	PaaS		

Use Standard Hardening Configuration Templates for Application Infrastructure

Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

Safeguard 16.8	Network	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Separate Production and Non-Production Systems

Maintain separate environments for production and non-production systems.

Safeguard 16.9	Users	Protect		IG2	IG3	IaaS	PaaS		FaaS

Train Developers in Application Security Concepts and Secure Coding

Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 16.10	Software	Protect		IG2	IG3	IaaS	PaaS		FaaS

Apply Secure Design Principles in Application Architectures

Apply secure design principles in application architectures including the security of APIs involved. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

Safeguard 16.11	Software	Protect		IG2	IG3	IaaS	PaaS		

Leverage Vetted Modules or Services for Application Security Components

Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

Safeguard 16.12	Software	Protect			IG3	IaaS	PaaS		FaaS

Implement Code-Level Security Checks

Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

Safeguard 16.13	Software	Detect			IG3	IaaS	PaaS	SaaS	

Conduct Application Penetration Testing

Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

Safeguard 16.14	Software	Protect			IG3	IaaS	PaaS		FaaS

Conduct Threat Modeling

Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

- **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 application software security. The CSP is only 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 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 your 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 that are needed to run applications and systems are safeguarded, as exposed secrets can put your systems at risk.

CONTROL 17

Incident Response Management

Overview

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Cloud Applicability

This CIS 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 our way 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 17.1	Users	Respond	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Designate Personnel to Manage Incident Handling

Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 17.2	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain Contact Information for Reporting Security Incidents

Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service providers, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 17.3	Documentation	Govern	IG1	IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain an Enterprise Process for Reporting Incidents

Establish and maintain a documented enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.4	Documentation	Govern		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain an Incident Response Process

Establish and maintain a documented incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.5	Users	Respond		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Assign Key Roles and Responsibilities

Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, analysts, and relevant third parties Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.6	Users	Respond		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Define Mechanisms for Communicating During Incident Response

Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, secure chat, or notification letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.7	Users	Recover		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Conduct Routine Incident Response Exercises

Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum.

Safeguard 17.8	Users	Recover		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Conduct Post-Incident Reviews

Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Safeguard 17.9	Documentation	Recover			IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain Security Incident Thresholds

Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include, abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

Incident response and management is no different in the cloud. If you have process and procedures in place organizationally, 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 you will have 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 must be taken into consideration to identify the areas to be focused upon and those that would primarily fall within the customer’s realm of responsibility.

CONTROL 18

Penetration Testing

Overview

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Cloud Applicability

This CIS 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.

As outlined in the Controls, penetration tests can provide significant value and improvement, but only when basic defensive measures are already in place and when these tests are performed as part of a comprehensive, ongoing security management program. 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.

Safeguards

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 18.1	Documentation	Govern		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Establish and Maintain a Penetration Testing Program

Establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

Number/Title	Asset Type	Security Function	Implementation Groups			Applicability of Service Model			
Safeguard 18.2	Network	Detect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Perform Periodic External Penetration Tests

Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

Safeguard 18.3	Network	Protect		IG2	IG3	IaaS	PaaS	SaaS	FaaS

Remediate Penetration Test Findings

Remediate penetration test findings based on the enterprise's documented vulnerability remediation process. This should include determining a timeline and level of effort based on the impact and prioritization of each identified finding.

Safeguard 18.4	Network	Protect			IG3	IaaS	PaaS	SaaS	FaaS

Validate Security Measures

Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.

Safeguard 18.5	Network	Detect			IG3	IaaS	PaaS	SaaS	FaaS

Perform Periodic Internal Penetration Tests

Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

Cloud Service and Deployment Considerations

When considering deployment models, you will find that this CIS Control and Safeguards are applicable for Private (on-prem). For Private (third-party hosted), Public, and Hybrid deployment models, you will need to defer to the service/deployment model(s) your enterprise is using.

Pen testing is no different in the cloud. If you have process and procedures in place organizationally, 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 you will have 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 center 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 center.
- While you may need permission to test from the FaaS service provider, 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.

Appendices

Appendix A

Abbreviations and Acronyms

AAA	Authentication, Authorization, and Auditing
API	Application Program Interface
AoC	Attestation of Compliance
CASB	Cloud Access Security Broker
CIS	Center for Internet Security
CSP	Cloud Service Provider
CWPP	Cloud Workload Protection Platforms
DEP	Data Execution Prevention
DevSecOps	Development, Security, and Operations, Automats the Integration of Security
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication Reporting, and Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
EDR	Endpoint Detection and Response
FaaS	Function as a Service
GDPR	General Data Protection Regulation
HSM	Hardware Security Model
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IDS	Intrusion Detection Systems
IG	Implementation Group
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MDM	Mobile Device Management
MFA	Multifactor Authentication
NaaS	Network as a Service
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevent System
NIS	National Intelligence Service
OpenSSH	Open Secure Shell
OT	Operational Technology
PaaS	Platform as a Service
PCI	Payment Card Industry
RBAC	Role-Based Access Control
SaaS	Software as a Service
SIEM	Security Information and Event Management
SIP	System Integrity Protection
SLA	Service-Level Agreements
SOC2	Service Organization Control 2
SPF	Sender Policy Framework
SSH	Secure Shell
SSO	Single Sign On
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access 2

Appendix B

Links and Resources

- CIS Controls: https://www.cisecurity.org/controls/
- https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-316.pdf
- https://iasecontent.disa.mil/cloud/SRG/index.html
- https://aws.amazon.com/types-of-cloud-computing/
- https://azure.microsoft.com/en-us/overview/what-is-paas/
- https://azure.microsoft.com/en-us/overview/what-is-a-private-cloud/
- https://azure.microsoft.com/en-us/overview/what-is-a-public-cloud/
- https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/
- https://azure.microsoft.com/en-us/overview/what-is-a-private-cloud/
- https://azure.microsoft.com/en-us/overview/serverless-computing/
- https://www.redhat.com/en/topics/cloud-computing/what-is-public-cloud
- https://www.redhat.com/en/topics/cloud-computing/what-is-private-cloud
- http://www.cloudgarage.in/cloud-services/hybrid/
- https://www.webopedia.com/TERM/P/public_cloud.html
- https://www.liquidweb.com/kb/difference-private-cloud-premise/
- https://www.techopedia.com/definition/26559/community-cloud
- https://www.eci.com/cloudforum/private-cloud-explained.html
- https://www.ibm.com/cloud/learn/iaas-paas-saas
- https://medium.com/@BoweiHan/an-introduction-to-serverless-and-faas-functions-as-a-service-fb5cec0417b2
- Gartner's Market Guide for Cloud Workload Protection Platforms

Appendix C

Information

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 8 to cloud environments. You can find the newest version of the CIS Controls and other complementary documents at www.cisecurity.org.

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and for assistance in creating cybersecurity guidance. If you are interested in volunteering or if you have questions, comments, or have identified ways to improve this guide, please contact us at controlsinfo@cisecurity.org.

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact

Center for Internet Security
31 Tech Valley Drive
East Greenbush, NY 12061
518–266–3460
controlsinfo@cisecurity.org

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CIS® Center for Internet Security®

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security

CenterforIntSec
@CISecurity
TheCISecurity
cisecurity