



Version 7

# CIS Critical Security Controls® (CIS Controls®) Cloud Companion Guide

## Contents

Acknowledgments.....	2
Introduction .....	3
How to Use This Document.....	6
CIS Controls (Version 7): Cloud Security .....	7-60
References.....	61

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

To further clarify the Creative Commons license related to the CIS Controls™ content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization, for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (<http://www.cisecurity.org/controls/>) when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of CIS® (Center for Internet Security, Inc.®).

## Acknowledgments

CIS® (Center for Internet Security, Inc.®) 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  
Robin Regnier

### Contributors:

Kesten Broughton, Praetorian Senior Security Engineer  
Tyler Desjardins, CISSP  
Jason Hulling, IBM Cloud Senior Security Architect  
Staffan Huslid, knowit Secure Senior Security Advisory  
Tony Krzyzewski, SAM for Compliance Ltd Director  
Hardeep Mehrotara, CISSP, CISA, GSEC, ISMSA. CICP  
David B. Pickens, CISM  
Tim J. Sandage, AWS Senior Security Partner Strategist  
James Tarala, Information Security Specialist  
Jonathan C. Trull

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

## Introduction

The 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 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. So, while the CIS Controls address the general practices that most organizations should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls.

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 organization’s infrastructure.

The Center for Internet Security, Inc. (CIS) is a 501(c)(3) nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cybersecurity; deliver world-class cybersecurity solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.

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

Rather than chase every new exceptional threat and neglect the fundamentals, how can we get on track with a roadmap of fundamentals and guidance for measures and improve? How can we get on track with a roadmap of fundamentals, and guidance to measure and improve cloud security? Which CIS Controls and defensive steps are applicable and have the greatest value?

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 this 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 Information Technology (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 whom the assumed security risk resides with. 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 organization's security and management needs. Company management processes should ensure there is overlap rather than gaps in coverage between native and third-party tools.

A cloud environment has four distinct service models that the application or service can fall under:

- IaaS (Infrastructure as a Service) is a cloud environment that computing resources such as virtual servers, storage, and networking hardware. The consumer utilizes their own software such as operating systems, middleware, and applications. The underlying cloud infrastructure is managed by the CSP.
- PaaS (Platform as a Service) is a cloud computing environment for development and management of a consumer's applications. It includes the infrastructure hardware: virtual servers, storage, and networking while tying in the middleware and development tools to allow the consumer to deploy their applications. It is designed to support the complete application lifecycle while leaving the management of the underlying infrastructure to the CSP.
- 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 by one consumer (organization) 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 and applications that require complete control and configurability.
- Private cloud (third-party hosted) is a private cloud that is hosted by an external third party provider. The third party provides an exclusive cloud environment for the consumer and manages the hardware. All costs associated with the maintenance is the responsibility of the consumer.
- Community cloud (shared) is a deployment solution where the computing resources and infrastructure are shared between several organizations. The resources can be managed internally or by a third party and they can be hosted on-prem or externally. The organizations share the cost and often have similar cloud security requirements and business objectives.
- Public cloud is an infrastructure and computing services hosted by a third party company defined as a CSP. It is available over the internet and the services are delivered through a self-service portal. The consumer is provided on-demand accessibility and scalability

without the high overhead cost of maintaining the physical hardware and software. The CSP is responsible for the management and maintenance of the system while the consumer pays only for resources they use.

- Hybrid cloud is an environment that uses a combination of the three cloud deployment models, private cloud (on-prem), private cloud (third- party hosted), and public cloud with an orchestration service between the three deployment models.

These are the kinds of issues that led to and now drive the CIS Controls Cloud Companion Guide, <https://www.cisecurity.org/resources/white-papers/?o=controls>.

## How to Use This Document

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 7 to any cloud environment from the consumer/customer perspective. For each top-level CIS Control, there is a brief discussion of how to interpret and apply the CIS Control in such environments, along with any unique considerations or differences from common IT environments.

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

By walking through CIS Controls Version 7 with this companion guide, the reader should be able to tailor the CIS Controls in the context of a specific IT/OT cloud enterprise as an essential starting point for a security improvement assessment and roadmap.

### Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs




### Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

### Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

## Applicability Overview for each Service Model

	More than 60% of CIS Sub-Controls Apply
	Between 60% and 0% of the CIS Sub-Controls Apply
	0%

Applicability of Service Model					
Control	Control Title	IaaS	PaaS	SaaS	FaaS
1	Inventory and Control of Hardware Assets				
2	Inventory and Control of Software Assets				
3	Continuous Vulnerability Management				
4	Controlled Use of Administrative Privileges				
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers				
6	Maintenance, Monitoring and Analysis of Audit Logs				
7	Email and Web Browser Protections				
8	Malware Defenses				
9	Limitation and Control of Network Ports, Protocols, and Services				
10	Data Recovery Capabilities				
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches				
12	Boundary Defense				
13	Data Protection				
14	Controlled Access Based on the Need to Know				
15	Wireless Access Control				
16	Account Monitoring and Control				
17	Implement a Security Awareness and Training Program				
18	Application Software Security				
19	Incident Response and Management				
20	Penetration Tests and Red Team Exercises				

## CIS Control 1: Inventory and Control of Hardware Assets

*Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.*

### Cloud Rationale

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.

### Cloud Applicability

CIS Control 1: Inventory and Control of Hardware Assets					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	•	•		
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	•	•		
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	•	•		
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.	•	•		
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	•	•		



CIS Control 1: Inventory and Control of Hardware Assets					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	•	•		
1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	•	•		
1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	•		•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- 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, 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 — The administrator (cloud consumer) should consider utilizing client certificates to authenticate.
- FaaS — The administrator (cloud consumer) should consider utilizing client certificates to authenticate.

### 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.
- 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.
- In a Private cloud, it is very likely that the organization has full management control of the routing and switching, and CIS Sub-Control 1.7 may be implemented. In a Public cloud deployment model, implementing Sub-Control 1.7 is not feasible.

## CIS Control 2: Inventory and Control of Software Assets

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

### Cloud Rationale

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.

### Cloud Applicability

CIS Control 2: Inventory and Control of Software Assets					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	•	•	•	•
2.2	Applications	Identify	Ensure Software Is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	•	•	•	
2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	•	•		
2.4	Applications	Identify	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	•	•	•	
2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	•	•		
2.6	Applications	Respond	Address Unapproved Software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	•	•		

CIS Control 2: Inventory and Control of Software Assets					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
2.7	Applications	Protect	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	•			
2.8	Applications	Protect	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.	•			
2.9	Applications	Protect	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.	•			
2.10	Applications	Protect	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.	•			

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem — The local administrator is responsible for keeping the inventory of all software utilized regardless of the service model.
- IaaS — The administrator (cloud consumer) deploys, operates, and maintains the software utilized within this service model but does not manage the underlying cloud software 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 to make sure the vendor maintains support and vulnerability updates for the software and to keep record of it in the tracking software. 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.

## CIS Control 3: Continuous Vulnerability Management

*Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.*

### Cloud Rationale

This CIS Control addresses the need for continuous vulnerability management, which can be a significant task in most organizations. Understanding and managing vulnerabilities in a cloud environment can be more challenging than traditional IT systems. A cloud environment is dynamic, allowing you to scale your environment at an ever-changing pace. With the increasing use of DevOps and SecOps, 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.

### Cloud Applicability

CIS Control 3: Continuous Vulnerability Management					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	•	•		
3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	•	•		
3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	•	•		
3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	•	•		

CIS Control 3: Continuous Vulnerability Management					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	•	•		
3.6	Applications	Respond	Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	•	•		
3.7	Applications	Respond	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	•	•		

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem – The administrator (cloud consumer) is responsible for continuous vulnerability management of the hardware and software, both physical and virtual servers, networking, middleware, and applications utilized.
- IaaS -- The administrator (cloud consumer) is responsible for continuous vulnerability management of the software, virtual servers, virtual networking, middleware, and applications utilized. The CSP is responsible for continuous vulnerability management with the infrastructure and technology that they provide.
- PaaS -- The administrator (cloud consumer) is responsible for continuous vulnerability management of the applications and development tools utilized. The CSP is responsible for continuous vulnerability management of the hardware infrastructure and software technology that they provide.
- SaaS – This is not applicable for the cloud consumer. The CSP is responsible for everything but the data.
- FaaS – This is not applicable for the cloud consumer. The CSP is responsible for everything but the code and the data utilized within the functions.

### 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 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.



## CIS Control 4: Controlled Use of Administrative Privileges

*The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

### Cloud Rationale

This CIS Control addresses the need for limiting and managing administrator access. The misuse of administrative privileges is a primary method for attackers to spread 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, or 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. If administrative 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.

### Cloud Applicability

CIS Control 4: Controlled Use of Administrative Privileges					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
4.1	Users	Detect	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	•	•	•	•
4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	•	•	•	•
4.3	Users	Protect	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities.	•	•	•	•

CIS Control 4: Controlled Use of Administrative Privileges					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
4.4	Users	Protect	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	•	•	•	•
4.5	Users	Protect	Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.	•	•	•	•
4.6	Users	Protect	Use Dedicated Workstations for All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading email, composing documents, or browsing the Internet.	•	•	•	•
4.7	Users	Protect	Limit Access to Scripting Tools	Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.	•	•		
4.8	Users	Detect	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	•	•	•	•
4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	•	•	•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem -- The administrator (cloud consumer) is responsible for all account administration and administrator access.
- IaaS -- The administrator (cloud consumer) is responsible for administrator account management for the software, virtual servers, virtual networking, middleware, and applications utilized.
- PaaS -- The administrator (cloud consumer) is responsible for all administrator account management for the applications and development tools utilized.
- SaaS -- The administrator (cloud consumer) is responsible for all administrator accounts for the software service utilized. When inventorying all administrative accounts, automated tools are recommended but not applicable for all SaaS service models unless administrative access is managed outside the service.
- FaaS -- The administrator (cloud consumer) is responsible for all administrator accounts that utilize and manage the code and setup of the functions. When inventorying all administrative accounts, automated tools are recommended but not applicable for FaaS service models unless administrative access is managed outside the service.

### Cloud Additional Considerations

- Minimize the use of elevated privileges and only use administrative accounts where they are required. Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
- Account validation is performed by a system owner as opposed to a senior executive.
- The use of multi-factor authentication should be applicable to all service models when it can be used with the software, application, service, or systems.
- Default accounts that require administrative access and risks associated with altering those accounts should be reviewed and all changes verified with the vendor prior to making changes.

## CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

*Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.*

### Cloud Rationale

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.

### Cloud Applicability

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
5.1	Applications	Protect	Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.	•	•	•	•
5.2	Applications	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	•			
5.3	Applications	Protect	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	•			

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
5.4	Applications	Protect	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	•			
5.5	Applications	Detect	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	•	•		

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem -- The administrator (cloud consumer) is responsible for the use of a security baseline for all physical and virtual systems, software, and applications.
- IaaS -- The administrator (cloud consumer) is responsible for utilizing a security baseline for the software, virtual servers, virtual networking, middleware, and applications in the cloud environment.
- PaaS -- The administrator (cloud consumer) is responsible for utilizing a security baseline for the applications and development tools utilized.
- SaaS -- The administrator (cloud consumer) is responsible for a security baseline within the software and the data that is being utilized.
- FaaS -- The administrator (cloud consumer) is responsible for a security baseline within the code and the data being utilized.

### Cloud Additional Considerations

- When configuration management tools are used, they should be set to alert-only without automated configuration re-deployment unless it is known to be safe to do so.
- The CSP hosts typical image storage in cloud environments for PaaS, SaaS, and FaaS; therefore, the secure configuration of the underlying servers is the responsibility of the CSP.
- As part of the established secure configurations, SaaS and FaaS should always communicate over transport layer security (TLS) and validate the TLS API endpoint cert.

## CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

*Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.*

### Cloud Rationale

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.

### Cloud Applicability

CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
6.1	Network	Detect	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	•			
6.2	Network	Detect	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.	•	•		
6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	•	•	•	•
6.4	Network	Detect	Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.	•	•	•	•
6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	•	•	•	•
6.6	Network	Detect	Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis	•	•	•	•

CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	•	•	•	•
6.8	Network	Detect	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	•	•	•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem -- The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and process analysis 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 Sub-Controls.
- 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.

## CIS Control 7: Email and Web Browser Protections

*Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.*

### Cloud Rationale

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.

### Cloud Applicability

CIS Control 7: Email and Web Browser Protections					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
7.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	•	•	•	•
7.2	Applications	Protect	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	•	•	•	•
7.3	Applications	Protect	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	•	•	•	•
7.4	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	•	•		



CIS Control 7: Email and Web Browser Protections					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
7.5	Network	Protect	Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	•	•		
7.6	Network	Detect	Log All URL Requests	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	•	•		
7.7	Network	Protect	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	•	•		
7.8	Network	Protect	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	•	•		
7.9	Network	Protect	Block Unnecessary File Types	Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	•	•		
7.10	Network	Protect	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	•	•		

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem -- The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the email and web browser security.
- IaaS -- The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the email and web browser for the software, virtual servers, virtual networking, middleware, and applications when applicable in the cloud environment.

- PaaS -- The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the email and web browser capabilities for the applications, operating systems, and development tools utilized when applicable.
- SaaS -- The administrator (cloud consumer) is responsible for email and web browser security.
- FaaS -- The administrator (cloud consumer) is responsible for email and web browser security.

#### Cloud Additional Considerations

- Sub-Control 7.8, 7.9, and 7.10 are only applicable if you are running an email server in your cloud-hosted environment with on-prem, IaaS, or PaaS services.
- The rest of the Sub-Controls 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 Flash or Java should be updated and the highest possible security policies should be applied according to your organizational requirements.
- Ensure that no email clients are installed or present on any systems. Where a device or system has the capability to send email-based alerts or reports, ensure that it is limited to outbound only.

## CIS Control 8: Malware Defenses

*Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.*

### Cloud Rationale

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. Unfortunately, the ability to collaborate, sync, and share—the same reasons consumers migrate to the cloud—are the reason that malware can spread quickly and can cause greater damage.

### Cloud Applicability

CIS Control 8: Malware Defenses					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
8.1	Devices	Protect	Utilize Centrally Managed Anti-Malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	•	•		
8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	•	•		
8.3	Devices	Detect	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	•	•		
8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Media	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	•			

CIS Control 8: Malware Defenses					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
8.5	Devices	Protect	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.	•			
8.6	Devices	Detect	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	•	•		
8.7	Network	Detect	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	•	•		
8.8	Devices	Detect	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	•	•		

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem -- The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the anti-malware software and other security settings for all physical and virtual devices in place to prevent any intrusions.
- IaaS -- The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the anti-malware software and other security settings for the software, virtual servers, virtual networking, middleware, and applications when applicable in the cloud environment.
- PaaS -- The administrator (cloud consumer) is responsible for the setup, maintenance, monitoring, and analysis of the anti-malware software and other security settings for the applications, operating systems, and development tools utilized when applicable.
- SaaS -- This Control and all of its Sub-Controls is not applicable for the cloud consumer.
- FaaS -- This Control and all of its Sub-Controls is 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.

## CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

*Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.*

### Cloud Rationale

This CIS Control focuses on the need for controlling network access points, ports, and services. When accounting for ports, protocols, and services, it is recommended to start with CSP documentation. This cloud network should contain details specific to the service solutions you are using.

### Cloud Applicability

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
9.1	Devices	Identify	Associate Active Ports, Services, and Protocols to Asset Inventory	Associate active ports, services, and protocols to the hardware assets in the asset inventory.	•			
9.2	Devices	Protect	Ensure Only Approved Ports, Protocols, and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.	•	•	•	•
9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	•	•	•	•
9.4	Devices	Protect	Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	•	•		
9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	•	•	•	

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem -- The administrator (cloud consumer) is responsible for managing (track/control/correct) the ongoing operational use of ports, protocols, and services for all physical and virtual devices, and applications to minimize and prevent any intrusions.
- IaaS -- The administrator (cloud consumer) is responsible for managing (track/control/correct) the ongoing operational use of ports, protocols, and services for all software, virtual servers, virtual networking, middleware, and applications when applicable in the cloud environment.
- PaaS -- The administrator (cloud consumer) is responsible for managing (track/control/correct) the ongoing operational use of ports, protocols, and services for all applications, hosting operating systems environment settings, and developing the tools utilized.
- SaaS -- The administrator (cloud consumer) is responsible for managing (track/control/correct) the ongoing operational use of ports and some protocols, and services for the application/software that is running as a service in the cloud environment. In addition, SaaS might have specific port requirements to function so these have to be monitored for any changes.
- FaaS -- The administrator (cloud consumer) is responsible for managing (track/control/correct) the ongoing operational use of ports and some protocols as some of the functions or code affecting the specific actions or workflow will be dependent on those ports and protocols.

### Cloud Additional Considerations

- When inventorying open or available network ports, the process or tools used should be non-intrusive and not affect the availability or reliability of the cloud systems or environment.

## CIS Control 10: Data Recovery Capabilities

*The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.*

### Cloud Rationale

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 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.

### Cloud Applicability

CIS Control 10: Data Recovery Capabilities					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
10.1	Data	Protect	Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.	•	•	•	•
10.2	Data	Protect	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	•	•		
10.3	Data	Protect	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	•	•	•	•
10.4	Data	Protect	Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	•	•	•	•
10.5	Data	Protect	Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.	•	•	•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem -- The administrator (cloud consumer) is responsible for all data recovery capabilities in the environment.
- IaaS -- The administrator (cloud consumer) is responsible for data recovery capabilities for all software, virtual servers, virtual networking, middleware, and applications when 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. Sub-Control 10.2 is not applicable to a SaaS service model as you are not able to back up a complete system while providing an image or a process such as imaging for recovery.
- 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. Sub-Control 10.2 is not applicable to a FaaS service model as you are not able to back up a complete system while providing an image or a process such as imaging for recovery.

### Cloud Additional Considerations

- When referencing system data, be sure to include user data in that context. This inclusion is what makes this CIS Control and the majority of the CIS Sub-Controls 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.



## CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

*Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.*

### Cloud Rationale

This CIS Control addresses the need to manage the configuration of all network devices using a change control process. 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.

### Cloud Applicability

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain documented security configuration standards for all authorized network devices.	•	•		
11.2	Network	Identify	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	•	•		
11.3	Network	Detect	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered.	•	•		

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	Paas	SaaS	FaaS
11.4	Network	Protect	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.	•			
11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.	•			
11.6	Network	Protect	Use Dedicated Workstations for All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.	•			
11.7	Network	Protect	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	•			

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

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

- PaaS -- The administrator (cloud consumer) manages the application, 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.
- Anytime multi-factor requirements can be applied will help maintain accountability and configuration management.

## CIS Control 12: Boundary Defense

*Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.*

### Cloud Rationale

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 the multi-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.

### Cloud Applicability

CIS Control 12: Boundary Defense					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
12.1	Network	Identify	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	•			
12.2	Network	Detect	Scan for Unauthorized Connections Across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	•			
12.3	Network	Protect	Deny Communications With Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.	•	•		
12.4	Network	Protect	Deny Communication Over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	•	•		

CIS Control 12: Boundary Defense					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
12.5	Network	Detect	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	•			
12.6	Network	Detect	Deploy Network-Based IDS Sensors	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	•			
12.7	Network	Protect	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	•			
12.8	Network	Detect	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	•			
12.9	Network	Detect	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	•			
12.10	Network	Detect	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	•			
12.11	Users	Protect	Require All Remote Logins to Use Multi-Factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	•			
12.12	Devices	Protect	Manage All Devices Remotely Logging Into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	•			

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- On-prem -- The administrator (cloud consumer) is responsible for the network boundary 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 and operating systems and the development tools utilized to apply some deny communications, as outlined in Sub-Controls 12.3 and 12.4.
- SaaS -- This is not applicable to the cloud consumer. The CSP would be responsible for the boundary defense.
- FaaS -- This is 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.

## CIS Control 13: Data Protection

*The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.*

### Cloud Rationale

This CIS Control's focus 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.

### Cloud Applicability

CIS Control 13: Data Protection					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
13.1	Data	Identify	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	•	•	•	•
13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	•	•	•	
13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	•	•		
13.4	Data	Protect	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	•	•		

CIS Control 13: Data Protection					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	•	•		
13.6	Data	Protect	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.				
13.7	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.				
13.8	Data	Protect	Manage System's External Removable Media's Read/Write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	•			
13.9	Data	Protect	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.				

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- 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.

## CIS Control 14: Controlled Access Based on the Need to Know

*The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.*

### Cloud Rationale

The focus of this CIS Control is around the process and tools used to determine which users, systems, and applications have the need and right to access critical data based on its classification. Consideration needs to be given to asset control lists (ACLs), virtual local area networks (VLANs), security groups, and other security in the CSP to control access and other routing requirements. There are many references to sensitive data throughout this Control. These references should align with CIS Control 13, Data Protection. This reference may remove applicable parts of this Control depending on the cloud service and deployment model utilized.

### Cloud Applicability

CIS Control 14: Controlled Access Based on the Need to Know					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
14.1	Network	Protect	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	•			
14.2	Network	Protect	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	•			
14.3	Network	Protect	Disable Workstation-to-Workstation Communication	Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as private VLANs or micro segmentation.	•			

CIS Control 14: Controlled Access Based on the Need to Know					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
14.4	Data	Protect	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	•	•	•	•
14.5	Data	Detect	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.	•			
14.6	Data	Protect	Protect Information Through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•	
14.7	Data	Protect	Enforce Access Control to Data Through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when the data is copied off a system.	•			
14.8	Data	Protect	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	•	•		
14.9	Data	Detect	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	•	•		

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- Private (on-prem) -- The administrator (cloud consumer) is responsible for all access regardless of the service model used.
- IaaS -- The administrator (cloud consumer) is responsible for access to the virtual networks, virtual machines applications, the consumer account, and data protection within this service model. The CSP is not responsible for this access at the cloud consumer account level.
- PaaS -- The administrator (cloud consumer) manages the access control for the applications and in some cases the host environment settings and operating systems.
- SaaS -- The administrator (cloud consumer) is responsible for the application and data access. 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 consumer.
- FaaS -- The administrator (cloud consumer) is responsible for the functional code and data access. 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 consumer.

### Cloud Additional Considerations

- For organizations operating in the cloud, it is important to understand the security controls applied to data in the cloud multi-tenant environment, and determine the best course of action for application of encryption controls and security of keys.
- When possible, keys should be stored within secure containers such as Hardware Security Modules (HSMs).

## CIS Control 15: Wireless Access Control

*The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.*

### Cloud Rationale

This CIS Control references the security of wireless access points. Networks with wireless access points can be accessed from outside the physical building where security controls may be present. Likewise, rogue access points can be used to gain unrestricted access to internal systems and your environment. Due to the nature of cloud environments, wireless access controls fall under the physical controls outside of a cloud deployment and therefore they are not applicable.

### Cloud Applicability

CIS Control 15: Wireless Access Control					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
15.1	Network	Identify	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.				
15.2	Network	Detect	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.				
15.3	Network	Detect	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.				
15.4	Devices	Protect	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.				
15.5	Devices	Protect	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.				

CIS Control 15: Wireless Access Control					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
15.6	Devices	Protect	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.				
15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.				
15.8	Network	Protect	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.				
15.9	Devices	Protect	Disable Wireless Peripheral Access to Devices	Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.				
15.10	Network	Protect	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.				

When considering deployment models, you will find that this CIS Control and Sub-Controls are not applicable for Private (on-prem), Private (third-party hosted), Public, and Hybrid deployment models. You will need to defer to the service/deployment model(s) your organization is using.

### Cloud Considerations

For organizations operating in the cloud, Wireless Access Control (WAC) is not specific to that type of environment, and it will have most of its dependencies on the CIS Control and Sub-Control with reference to the physical operation of the organization.

## CIS Control 16: Account Monitoring and Control

*Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.*

### Cloud Rationale

This CIS Control focuses on managing the life cycle of system and application 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 organization or changes roles, a common vulnerability can arise if employee accounts are not closed or modified.

### Cloud Applicability

CIS Control 16: Account Monitoring and Control					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
16.1	Users	Identify	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.	•	•	•	•
16.2	Users	Protect	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	•	•	•	•
16.3	Users	Protect	Require Multi-Factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.	•	•	•	•
16.4	Users	Protect	Encrypt or Hash All Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.	•	•	•	•
16.5	Users	Protect	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	•	•		
16.6	Users	Identify	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	•	•	•	•

CIS Control 16: Account Monitoring and Control					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
16.7	Users	Protect	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	•	•	•	•
16.8	Users	Respond	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	•	•	•	•
16.9	Users	Respond	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	•	•	•	•
16.10	Users	Protect	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.	•	•	•	•
16.11	Users	Protect	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	•			
16.12	Users	Detect	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	•	•	•	•
16.13	Users	Detect	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.	•	•	•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- Private (on prem) -- The administrator (cloud consumer) is responsible for all accounts regardless of the service model used.
- IaaS -- The administrator (cloud consumer) is responsible for all accounts utilized on the virtual networks, virtual machines, applications, etc. The CSP is not responsible for this access at the cloud consumer account level.



- PaaS -- The administrator (cloud consumer) manages the accounts for the applications and in some cases the host operating systems.
- SaaS -- The administrator (cloud consumer) is responsible for the application accounts.
- FaaS -- The administrator (cloud consumer) is responsible for the accounts that have the ability to build the code execution based on the cloud functions.

#### Cloud Additional Considerations

- For consumers operating in the cloud, it is even more important to understand and maintain account control and inventory. The consumer is responsible for all the accounts and what level of access those accounts have to their cloud environment.
- When possible, multi-factor authentication should be required.
- The use of shared service accounts should be limited.
- Permissions should be granted through group membership, as that is easier to manage.
- The account principle of least privilege access should be followed.

## CIS Control 17: Implement a Security Awareness and Training Program

*For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.*

### Cloud Rationale

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 organization operating in the cloud.

### Cloud Applicability

CIS Control 17: Implement a Security Awareness and Training Program					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
17.1	N/A	N/A	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	•	•	•	•
17.2	N/A	N/A	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	•	•	•	•
17.3	N/A	N/A	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	•	•	•	•

CIS Control 17: Implement a Security Awareness and Training Program					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
17.4	N/A	N/A	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements.	•	•	•	•
17.5	N/A	N/A	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	•	•	•	•
17.6	N/A	N/A	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.	•	•	•	•
17.7	N/A	N/A	Train Workforce on Sensitive Data Handling	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.	•	•	•	•
17.8	N/A	N/A	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to <i>autocomplete</i> in email.	•	•	•	•
17.9	N/A	N/A	Train Workforce Members on Identifying and Reporting Incidents	Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.	•	•	•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### 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.

## CIS Control 18: Application Software Security

*Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.*

### Cloud Rationale

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.

### Cloud Applicability

CIS Control 18: Application Software Security					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
18.1	N/A	N/A	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.	•	•	•	•
18.2	N/A	N/A	Ensure That Explicit Error Checking Is Performed for All In-House Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	•	•	•	•
18.3	N/A	N/A	Verify That Acquired Software Is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	•	•	•	
18.4	N/A	N/A	Only Use Up-to-Date and Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.	•	•	•	

CIS Control 18: Application Software Security					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
18.5	N/A	N/A	Use only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized, currently accepted, and extensively reviewed encryption algorithms.	•	•	•	
18.6	N/A	N/A	Ensure Software Development Personnel Are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	•	•	•	•
18.7	N/A	N/A	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	•	•	•	
18.8	N/A	N/A	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	•	•	•	•
18.9	N/A	N/A	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	•	•	•	•
18.10	N/A	N/A	Deploy Web Application Firewalls	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	•	•	•	

CIS Control 18: Application Software Security					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
18.11	N/A	N/A	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	•	•	•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

#### Cloud Considerations

- Private (on-prem) -- The administrator (cloud consumer) is responsible for all application software security regardless of the service model used.
- IaaS -- The administrator (cloud consumer) is responsible for all application software security. The CSP will provide permission and access for scanning the cloud consumer software.
- PaaS -- The administrator (cloud consumer) manages the application software security for the applications and in some cases the host environment settings and operating systems. The CSP will provide permission and access for scanning the cloud consumer software.
- SaaS -- The administrator (cloud consumer) is responsible for the 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.

## CIS Control 19: Incident Response and Management

*Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.*

### Cloud Rationale

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 organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker’s presence, and recover in a secure fashion.

### Cloud Applicability

CIS Control 19: Incident Response and Management					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
19.1	N/A	N/A	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.	•	•	•	•
19.2	N/A	N/A	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation throughout the incident through resolution.	•	•	•	•
19.3	N/A	N/A	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	•	•	•	•

CIS Control 19: Incident Response and Management					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
19.4	N/A	N/A	Devise Organization-wide Standards For Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	•	•	•	•
19.5	N/A	N/A	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.	•	•	•	•
19.6	N/A	N/A	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.	•	•	•	•
19.7	N/A	N/A	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responder's technical capabilities using tools and data available to them.	•	•	•	•
19.8	N/A	N/A	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	•	•	•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.



### Cloud Considerations

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.

## CIS Control 20: Penetration Tests and Red Team Exercises

*Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.*

### Cloud Rationale

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.

Penetration tests can provide significant value, but only when basic defensive measures are already in place, and when these tests are performed as part of a comprehensive, ongoing program of security management, and improvement as outlined in the Controls. Each organization 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 organization's highest value information and production processing functionality.

### Cloud Applicability

CIS Control 20: Penetration Tests and Red Team Exercises					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
20.1	N/A	N/A	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	•	•	•	•
20.2	N/A	N/A	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	•	•	•	•

CIS Control 20: Penetration Tests and Red Team Exercises					Applicability of Service Model			
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	IaaS	PaaS	SaaS	FaaS
20.3	N/A	N/A	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	•	•	•	•
20.4	N/A	N/A	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.	•	•	•	•
20.5	N/A	N/A	Create a Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	•	•	•	•
20.6	N/A	N/A	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	•	•	•	•
20.7	N/A	N/A	Ensure Results From Penetration Test Are Documented Using Open, Machine-Readable Standards	Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	•	•	•	•
20.8	N/A	N/A	Control and Monitor Accounts Associated With Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	•	•	•	•

When considering deployment models, you will find that this CIS Control and Sub-Controls 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 organization is using.

### Cloud Considerations

- Running pen tests and Red Team exercises 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 the minimum the Reader + 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.

## Links and Resources

- CIS Controls - <https://www.cisecurity.org/controls/>
- [https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST\\_SP-500-291\\_Version-2\\_2013\\_June18\\_FINAL.pdf](https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf)
- [https://www.nist.gov/sites/default/files/documents/itl/cloud/CloudFrameworkSP500\\_316-2.pdf](https://www.nist.gov/sites/default/files/documents/itl/cloud/CloudFrameworkSP500_316-2.pdf)
- <https://iasecontent.disa.mil/cloud/SRG/index.html>
- <https://aws.amazon.com/types-of-cloud-computing/>
- <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>
- <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.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>

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 7 to cloud environments. You can find the newest version of the CIS Controls and other complementary documents at [www.cisecurity.org](http://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](mailto: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 Information

CIS  
31 Tech Valley Drive  
East Greenbush, NY 12061  
518.266.3460  
[controlsinfo@cisecurity.org](mailto:controlsinfo@cisecurity.org)