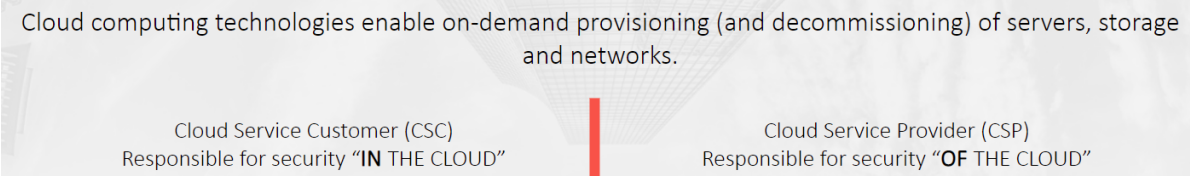
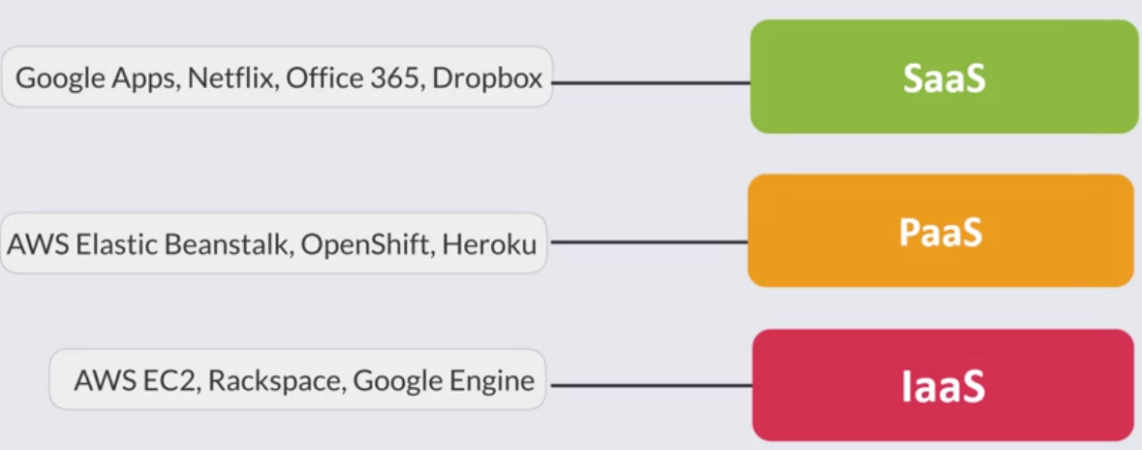
# Cloud Audit Academy - Cloud Agnostic Course

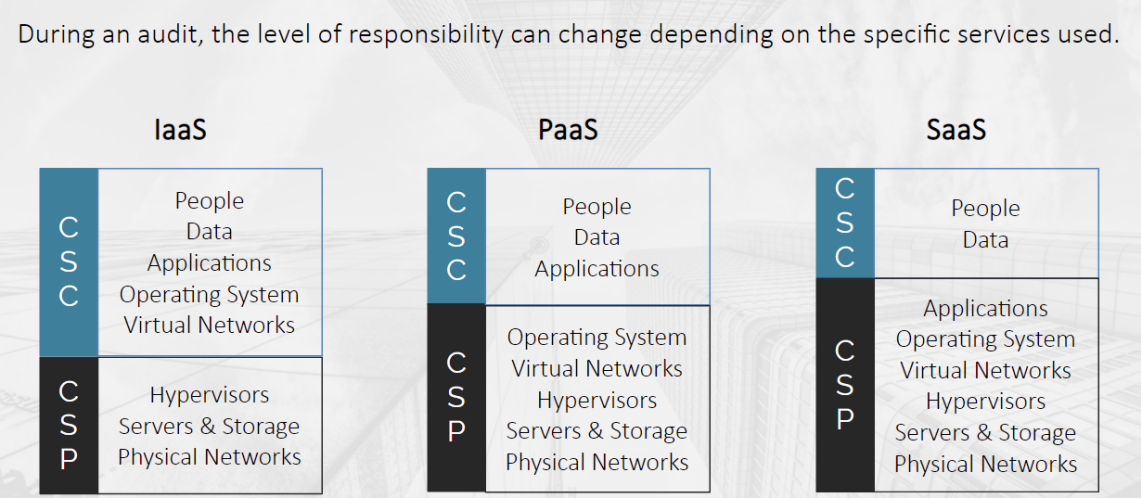
▼ Intro to Cloud Auditing




Service models:




Shared Responsibility by service:




Risk and benefits:

Benefits: inherited controls, visibility

Risk: misconfiguration, skills deficit

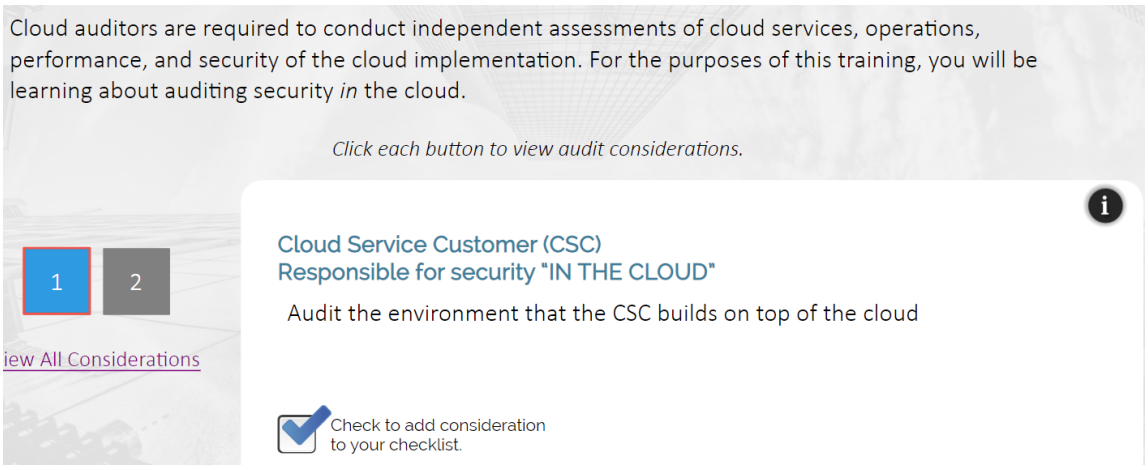
Cloud Focus

Cloud focus auditing refers to assessing the system specific controls (security *in* the cloud).

CSCs can leverage a CSP's third-party attestations as evidence or proof that the security requirements associated with the CSP have been satisfied. Depending on the CSP, CSCs can achieve continuous compliance through security services from their CSP instead of point in time assessments.

Applying cloud focus (security in the cloud) reduces duplicative audits that have already been completed by independent third-party auditors. Additionally, there are a wide variety of scopes when auditing cloud, from just a specific workload to enterprise cloud environments.

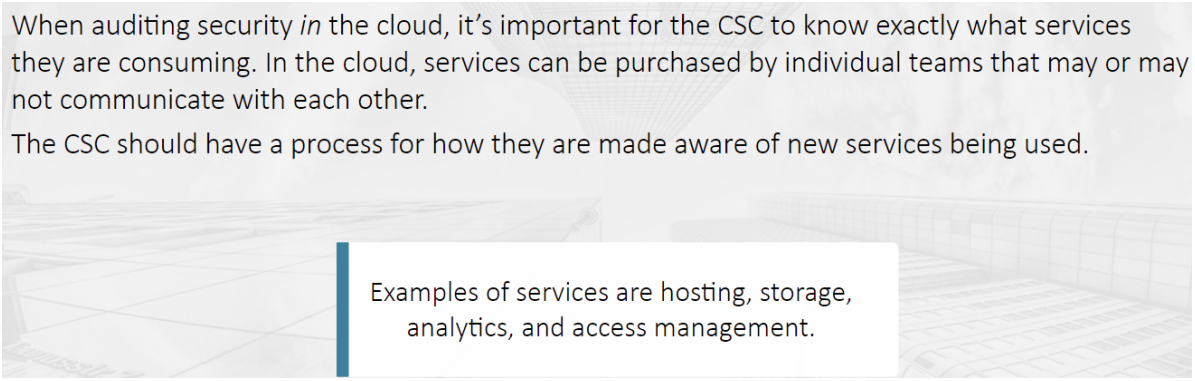
Scoping considerations




## Recap

- Cloud computing is a way to run applications, networks, and other resources like a utility service without having to manage a data center
- Security in the cloud pertains to the security measures a CSC implements and operates related to the security of CSC, it's content, and applications that make use of the CSP
- Security measures that the CSP implements and operates are the security *of* the cloud
- CSCs can leverage a CSP's third-party attestations as evidence or proof that the security requirements associated with the CSP have been satisfied

## ▼ Cloud services & scoping




## Service mapping

Service mapping in cloud environments illustrates the connections between all services the CSC uses. It helps to ensure appropriate security is in place for the entire environment.

In the cloud, offerings and consumption change frequently, so interdependencies can be impacted by deployments. Service mapping outlines dependencies for change management protocols.

## Focus

CSPs offer hundreds of services to CSCs. It is important to gain an understanding of what major CSP service types are being used and how their offerings can affect an audit.

This will allow you to verify that the services a CSC is consuming are, in fact, what they should be consuming to achieve their security objectives.

*Click the circle below to learn more.*

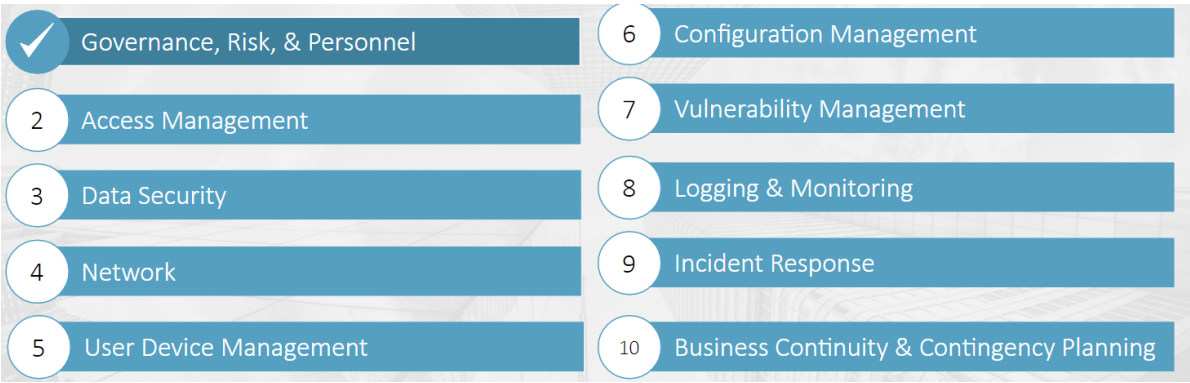

**All the services in use show up on the bill.**

It's important for CSCs to approach their cloud service "asset management" differently than on-premises, because it's dynamic. Assets can be provisioned and decommissioned in a matter of hours in the cloud, so having a real-time log of what is being used is essential.

## Recap

- It's important to gain an understanding of what major CSP service types are being used and how their offerings can affect an audit. This will allow you to verify that the services a CSC is consuming are in fact, what they should be consuming to achieve their security objectives.
- If mapping or inventory is not available, the bill is a place where all the services in use would show up.
- If a specific service is not "certified" as compliant with a particular framework it doesn't, necessarily, mean it isn't compliant in the CSC's implementation. In some cases, an CSC's additional security controls and design factors can result in the service's compliance.

## ▼ Security domains




## ▼ 1 Governance, Risk and Personnel

**Governance**, according to NIST CSF is the CSC's understanding of policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements and manage cyber security risk.

**Risk Assessment**, according to NIST CSF is the CSC understanding the cybersecurity risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

**Personnel Management**, according to NIST mentions that the CSC develops, documents, disseminates, and implements a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to its personnel and reviews and updates the current personnel security policy and procedures periodically.

These are the guard rails that keep cloud environments safe.

### Cloud governance focus

The difference between on-premises and in cloud auditing with regard to governance and oversight is that:

1. **Shared Responsibility**
   Some controls involve hand-offs between CSP and CSC. The assessment will be performed on the CSC policies, manuals, and other operational elements.
2. **CSP's Third-Party Attestations**
   Using the CSP's third-party attestations allow you to closely examine things that are under the responsibility of the CSP.
3. **CSP's Policy & Process Documentation**
   If you see policies and procedures that don't make sense for cloud technology, you can push back to see where they can be changed to reflect the current state, not simply reviewed and accepted annually. Obtain copies of the CSP's Policy & Process Documentation if available to ensure detailed alignment that may not be explicit in third-party attestation.

### Cloud risk focus


## Cloud focus personnel


## Recap

- When it comes to governance and oversight in the cloud, many controls are provided and owned by the CSP.
- If auditors see policies and procedures that don't make sense for cloud technology, they can push back to see where they can be changed to reflect the current state, not simply reviewed and accepted annually.
- Particularly when a CSC is a preliminary stage of migration, you want to be sure their use of cloud is reflected in their policies and procedures.

## ▼ 2 Access Mgmt

Access management is the process of identifying, tracking, controlling, and managing authorized or specified users' access to a system, application or any IT instance. The most important principle for the CSC to apply and for you to look for is *least privilege*.

*Least privilege refers to granting only the permissions required to perform a specific task.*

*Click the circle to learn more.*

Logical Access Controls

**Logical access controls determine access & type of actions.**
Logical access controls determine not only who, or what, can have access to a specific system resource, but also the type of actions that can be performed on the resource (read, write, etc.). As part of controlling access to resources, users and processes must present credentials to confirm that they are authorized to perform specific functions or have access to specific resources. The credentials required vary depending on the type of service and the access method, and include passwords, cryptographic keys, and certificates.

## Cloud focus

The difference in auditing cloud versus on-premises access management is that access management is a **shared responsibility** in the cloud

1. The CSP is responsible for controlling the identity and access "**of**" the cloud
2. The CSC is responsible for controlling the identity and access "**in**" the cloud

### Related Risk

A main risk is that a CSCs can leverage their root account to access cloud resources from anywhere and accidentally make changes to or delete cloud resources. Root access in the cloud is the ability to create or change any resource and any change you want in the environment.

**Root access best practice:** secure it then never use it again, and apply principle of least privilege to all access.

## CSC responsibilities

For security in the cloud, CSC access to cloud service provider (CSP) resources can be enabled through the CSP account, a CSP identity and access management system user account created under the CSP account, or identity federation with the CSC's corporate directory (single sign-on).

Using an access management system, a CSC can:

1. Enable users to securely control access to CSP services and resources
2. Create and manage users and groups and use permissions for access control
3. Control access to critical information and systems based on a need-to-know classification

## Recap

- An important concept in cloud security is that of least privilege. Simply stated, least priviledge means that every user or process is given the least amount of permissions required to achieve their assigned task.
- The difference in auditing cloud versus on-premises access management is that access management is a shared responsibility between the CSC and the CSP in the cloud.
- Using an access management system, a CSC can enable users to securely control access to CSP services and resources, create and manage CSP users and groups, and use permissions to allow and deny access to CSP resources.

## ▼ 3 Data Security

Data security is the design of an information system to classify data and ensure its confidentiality and integrity during handling.

### Data Classification Scheme

CSC should develop data classification scheme that defines what data is sensitive, confidential, and public. If the CSC does not appropriately classify data, it may not be possible to adequately address risks related to inappropriate user access.

### Data at Rest

Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way.

### Data in Transit

Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network.

### Key Management

Encryption involves the use of keys. Key management means protecting encryption keys from loss, corruption, and unauthorized access. Key-misalignment is one of the major risks in the cloud environment. For examples, key mis-management could result in data leakage, and coding mistakes made by a security administrator could result in a reputational risk for the CSC.

## Cloud Focus

The difference between on-premises and in cloud auditing with regard to data security is that:

1. Encryption and key management can be a shared responsibility for both the CSP and the CSC.
2. For data in transit – in the cloud, the data transmission process changes based on the cloud mode (where the data originates, passes through, and ends up). It is highly configurable, and routing can be specified within the CSP regions.
3. It is important for CSCs to know when it's their versus the CSP responsibility to encrypt, and if the CSP provided encryption is to their standards.

## Recap

- The cloud data transmission process changes based on the cloud mode, making it highly configurable. Data at rest should be encrypted as well as in flight for many regions.
- Encryption and key management can be a shared responsibility for both the CSP and the CSC.

## ▼ 4 Network

Network management is key to ensure efficiency and security of cloud environments. The difference between on-premises and in cloud auditing with regard to network management is that:

1. Network components such as firewalls and routers are virtual and function differently in the cloud environment. This virtual aspect allows for CSC to script and automate, which also means CSC can mis-configure it.

View Note on Virtual Firewall

2. Network configuration and architecture must follow the CSP security requirements with regards to the segregation of resources using subnets and routing tables, secure configuration of DNS, and limiting inbound and outbound traffic.
3. Each CSP may implement their underlying network differently, including network resilience and backup, and network routing that may include sending traffic over external or untrusted networks. These aspects may impact the appropriateness of the CSC virtual network implementation, including configuration for backup and resilience, security and encryption.

## CSC responsibilities

**ONE**
The virtual aspect of firewalls and routers allows for CSC to script and automate, which also means CSC can mis-configure it

**TWO**
CSP provides best practices for network configuration and architecture

**THREE**
Each CSP may implement their underlying network differently

1. The CSC should scope and manage rules for all traffic, since there could be any number of network entry points.
2. Firewall rules must be scoped for public internet traffic.
3. Security groups can be leveraged for network segmentation. Security groups filter all traffic to the service (internal to the CSC environment or external).

Note that traffic usually goes through the internet to access the services in the cloud. Even though a CSC is consuming services inside the cloud, auditors need to know the traffic routes, therefore, data flow diagrams are necessary.

1. The CSC must perform monitoring of their network, and can do so using host-based intrusion detection and monitoring systems.
2. A host-based intrusion detection system (HIDS) is a system that monitors a computer system on which it is installed to detect an intrusion and/or misuse, and responds by logging the activity and notifying the designated authority.
3. CSPs may offer DDoS protection. Leverage CSPs offered DDoS protection. DDoS attacks are designed to exhaust resources and bandwidth, denying service to legitimate users of the network.

1. Understand how data moves along the CSP subscribed services and within the CSC environment
2. Understand the connectivity with the cloud. For example, is there a VPN? With VPN connections, it is important to understand which networks the VPN connects between, for example an on- premises data center network and a cloud virtual network

To implement cloud infrastructure, most organizations use a virtual private cloud, which is an on-demand configurable pool of compute resources within a cloud environment that is isolated from other environments or organizations using the resources. It is essential to audit that the virtual network configuration is appropriate and as-desired.

## Recap

- Network configuration and architecture must follow the CSP security requirements.
- CSCs who must perform monitoring of their network, can do so using host-based intrusion detection and monitoring systems.
- In the cloud, ensuring the automated security controls and virtual network are configured properly is essential.

## ▼ 5 User device management

The difference between on-premises and in cloud auditing with regard to user device management is that:

1

A CSP still requires the end-user and workstations to be managed appropriately to prevent the infiltration of malicious code. Having the environment running in a third-party system with the infrastructure managed by other organizations, such as a CSP, does not eliminate a threat of incursion of malicious code.

2

It's easier for users to access the cloud from mobile devices via a standard internet connection. This makes it easier to get data into the cloud. CSC's don't have the same control when it comes to mobile devices. For example, a cloud back up service: unless you have control over each phone and don't allow users to back up automatically, you do not have full control. It all depends on the management profiles on the mobile devices and how they are managed.

3

Different network constructs (the interplay of different networks, bifurcation of the corporate network and production security boundary) impact security boundaries for user devices because user devices should ideally never connect directly to the production environment. You must evaluate this to understand if the user device configurations are compliant with requirements/policy (MDM Policy).

## Boundaries

Different network constructs impact **security boundaries** for user devices . Security boundaries are usually defined by a set of systems that are under a single administrative control. In the cloud, there is a separation between the device and the actual cloud environment. As an auditor, you need to understand where the boundaries are between production environments and user devices.

There are security boundaries between networks and devices. They generally fall into three categories:

- CSP employee user devices *(e.g. CSP developer terminal)*
- CSC user devices *(e.g. CSC employee mobile phone)*
- External user devices *(e.g. CSC customer desktop)*

With regards to enforcing user device configuration compliance with CSC requirements and policies, the CSC can sometimes leverage a cloud access security broker (CASB). A CASB is an on-premises or cloud-based security policy enforcement point between the CSC and the CSP. It addresses cloud service risks, enforces security policies, and complies with regulations, even when cloud services are beyond their perimeter and out of their direct control.

## Recap

- There is a separation between the device and the actual cloud environment. As an auditor, you need to understand where the boundaries are between production environments and user device.
- Best practices for user device management include:
  - Having a workflow diagram between user devices and network construct.
  - Having policies in place for BYOD and MDM.
  - Understanding the hand-off between the CSP and CSC.

# ▼ 6 Config mgmt

Configuration management (CM) is a governance and systems engineering process for ensuring consistency among physical and logical assets in an operational environment and guide software development lifecycles and change management. The goal is to identify and track individual configuration items (CIs), and document functional capabilities and interdependencies.

## Cloud focus

1. CSC should monitor the operating system and application security vulnerabilities to protect the security, stability, and integrity of the assets
2. Continuous Integration and Continuous Deployment (CI/CD) can significantly change how to audit change management in the cloud and the unique aspects of the pipeline workflow (and evidence) should be understood

## CSC responsibilities

CSC are responsible for maintaining the security of anything installed on CSP resources or connected to cloud resources. The assets themselves belong to and are assessed by the CSP. Often cloud servers are not included in the regular configuration management scope.

**Resource Tagging**

Resource tagging in the cloud ensures that a CSC can easily and methodically manage, search for, and control cloud resources by purpose, owner, environment, or other criteria.

*An example of the difference in the cloud is that for system hardening, a best practice is simply to wipe out and override image of a virtual machine versus patch a physical machine.*

**Configuration Templates**

Look at configuration templates instead of looking at each machine image, maximizing efficiency. Configuration templates provide the ability to standardize infrastructure components used across a CSC, enabling configuration compliance and faster troubleshooting as part of a CSC's configuration management solution.

## CI/CD

Continuous Integration and Continuous Deployment (CI/CD) can significantly change how to audit change management in the cloud and the unique aspects of the pipeline workflow (and evidence) should be understood. CICD pipelines in the cloud are setup to protect the environments and the code that a physical developer is pushing is actually published by the workflow.

**Change management looks different in the cloud.**

Change management *in* the cloud can be done in development and subsequently (and automatically) deployed downstream. To assess security, look at the entire environment, since it may not be easy to determine what hardware an application resides on if the focus is only one application. In the DevOps culture, any individual with permissions can make a change; these individuals can sit outside IT.

> DevOps is a culture shift in the IT world, it's a pairing of software development and information technology operations teams closely together. DevOps works closely with the business to shorten the systems development lifecycle while delivering features and updates frequently (e.g. daily or by the hour instead of sprints). It focuses on ensuring that software is continuously iterated and released reliably, with security in mind. The ultimate goal of DevOps is automation, moving processes that used to necessitate humans to rely on technology instead. DevOps still supports an agile release cycle.

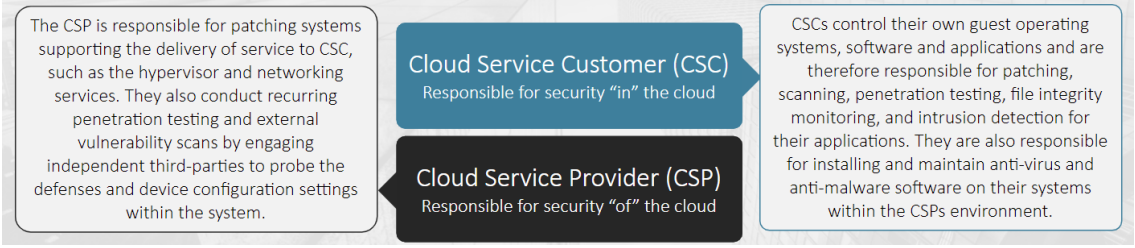
## Recap

- CSCs are responsible for maintaining the security of anything installed on CSP resources or connected to cloud resources. Secure configuration of resources also extends to the management of a CSP's asset inventory, configuration settings, patching and anti-malware are secure, and change management.
- DevOps is a culture shift in the IT world, it's a pairing of software development and information technology operations teams closely together.
- The difference in auditing cloud versus on-premises configuration management controls is that with cloud you are ensuring the CSC monitors operating system and application security vulnerabilities to protect the security, stability, and integrity of the assets, and the assets themselves belong to and are assessed by the CSP.

## ▼ 7 Vulnerability mgmt

Risks in the cloud typically look like a data breach, a takeover of cloud accounts to provision or use resources other than intended, insider threat, insecure APIs, etc. These are generally the result of insecurely configured cloud services, which is why it is important during audit to ensure that the CSC is testing and has configured their cloud services appropriately. Penetration in the cloud is of the virtual instances, networks, and applications.

*Click each button below to understand how this applies to the Shared Responsibility Model.*




## Scanning Tools

Traditional vulnerability scanning tools may not work in the cloud environment because the environment is so dynamic. It is necessary to assess provided cloud native assessment tools compared to third party tools to scan the CSC's dynamic environment. CSC should know if their data or the servers that they are running has an increased level of vulnerability and be able to respond accordingly. CSC should be able to respond and not just rely on the CSP.

### Related Risk

The most apparent risk of cloud versus on-premises from a threat vector perspective, is that attackers are more targeted at CSPs rather than individual data centers. It is imperative that the CSC configures their services securely and takes advantage of automated monitoring and logging to inform vulnerability management. The CSC must ensure they have the ability, policies, and capabilities to tune the environment to their specific risks.

## Cloud Focus

The difference in auditing in the cloud versus on-premises for vulnerabilities is that depending on the services being used, the delineation of the responsibility for vulnerability management may differ. However, vulnerability management will always be a shared responsibility between the CSP and CSC.

It is a common misconception that a CSP will perform all vulnerability management on behalf of the CSC, when in many cases the responsibility to patch systems is the CSC's responsibility. Identification of these services and tools is important to determine the scope of vulnerability needs to be audited and managed, or how much can be used through third-party attestations.

Vulnerability Management Best Practices:

| | | | |
|---|---|---|---|
| Patch management strategy *(controlling info flow into environment)* | Proactive detection *(performing pen testing)* | Virus detection *(deploying virus protection)* | Border definition *(defining the point where data passes to another network)* |

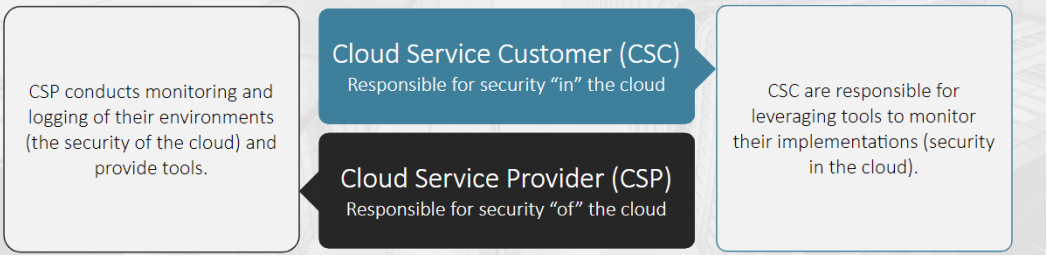
## Recap

- The delineation of the responsibility for vulnerability management may differ based on the type of service. However, vulnerability management will always be a shared responsibility between the CSP and CSC
- It is a common misconception that a CSP will perform all vulnerability management on behalf of the CSC, when in many cases the responsibility to patch systems is the CSC's responsibility.
- Best practices include: determine risks, identify vulnerabilities, check the scanning tools are working properly and how they are being used, review output, develop lessons learned and identify how the CSC is approaching patching, how they pen test, and how they are prioritizing vulnerabilities.

## ▼ 8 Logging & Monitoring

Logging and monitoring is an essential function of cloud security. It allows CSC and CSPs to review traffic patterns and look for anomalous and malicious activity to protect security. These monitoring activities and events inside and outside the information system and the logging of information pertinent to these activities can also be used to establish baselines for automated detection of possible security issues.

*It is essential for the CSC (and you) to understand the shared responsibility. Click each of the button below to learn more.*




## IDS and IPS

You can help determine if the tools the CSCs chose are the right ones, how the CSC is evaluating the CSP provided logs, and what they are doing with that information.

| Intrusion Detection Systems | Intrusion Prevention Systems |
|---|---|
| These systems monitor networks or individual systems for malicious activity or policy violations. The most common types are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). | These systems respond to malicious activity or policy violations. The systems used by the CSP are for security of the cloud and CSCs are responsible for their security in the cloud. |

Machine learning can be utilized to recognize good traffic versus malicious traffic via anomaly detection. The physical level of logging is not applicable for CSCs in the cloud. All data center management belongs to the CSP.
Security events should be monitored regardless of where the assets reside. You can assess consistency of controls across all environments, and validate full coverage through testing. Logs should NOT be changeable. The CSC should configure alerting and the monitoring element.

## Cloud focus

Auditing the cloud versus on-premises for logging and monitoring is actually the same, just without the physical level. The systems must be logged and monitored, just as they are for on-premises systems. CSC should collaborate with the CSP to evaluate and configure appropriate logs and thresholds for monitoring.

> *The biggest security risk for monitoring and logging is not identifying the ownership at an appropriate level, meaning that a CSC may think the CSP is doing something for them that is not actually happening. It is essential for the CSC and the CSP to understand the shared responsibility.*

## Recap

- The most common types of intrusion detection systems are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS).
- CSCs should collaborate with the CSPs to evaluate and configure appropriate logs and thresholds for monitoring.
- The biggest security risk for monitoring and logging is not identifying the ownership at an appropriate level, meaning that a CSC may think the CSP is doing something for them that is not actually happening.

## ▼ 9 Incident Response

Incident response is an organizational mechanism to respond to incidents, including initial reporting, information-gathering, root-cause analysis, remediation, and notification of stakeholders.

*Click on each button below to understand how this applies to the Shared Responsibility Model in general.*

The CSP detects and responds to events impacting the hypervisor and the underlying infrastructure.

**Cloud Service Customer (CSC)**
Responsible for security "in" the cloud

**Cloud Service Provider (CSP)**
Responsible for security "of" the cloud

CSC manage events from the guest operating system up through the application. You should understand incident response responsibilities and adapt existing security monitoring/alerting/audit tools and processes for the CSP resources.

## Cloud Focus

The difference in the cloud is that it's a joint partnership. If an infrastructure event happens and the CSP goes down, the CSC will work together to resolve the incident. Security events should be monitored regardless of where the assets reside. You can assess consistency of deploying incident management controls across all environments, and validate full coverage through testing.

An incident response plan should include:

| | | | |
|---|---|---|---|
| Communication path outlined between CSC and CSP | Notification procedures and how the CSC addresses responsibility for losses associated with attacks (CSP and CSC agreed upon SLAs) | CSC's recovery time objective (RTO) and recovery point objective (RPO) | Responsible, Accountable, Consulted, Informed (RACI) documentation |

## Recap

- Security events may be monitored by both CSP and the CSC. In the cloud responsibility for incident response is a joint partnership. If an infrastructure event happens and the CSP goes down, the CSC will work together to resolve the incident.
- The key attributes to an incident response plan are: Preparation, Identification or Detection, Containment, Investigation, Eradication, Recovery, and Follow-up.

## ▼ 10 Business continuity and contingency planning

Business continuity and contingency planning (BCP) are organizational safeguards and mechanisms that ensure the ongoing availability of information system functionality and access to data.

The difference between on-premises and in cloud auditing with regard to business continuity and contingency planning is that:

1. Architecting in a cloud-centric approach offers CSCs greater levels of business continuity than static CSC owned data centers, if deployed correctly.
2. CSCs must ensure that they configure systems that require high availability or quick recovery times to take advantage of the multiple regions.

### High Availability

CSPs provide a highly available infrastructure that allows CSCs to architect resilient applications and quickly respond to major incidents or disaster scenarios. This makes business continuity planning (BCP) typically better in the cloud than on-premises.

### Multi-Region Backups

Multi-region backups are also known as cross-region redundancy. Doing this is a disaster recovery best practice; ensuring that data is replicated in multiple places makes it always available in the unlikely event that it is lost in one region. For appropriate deployment, and assessment of this audit, it is critical that recommended multi-regions are used. While a cloud service provider may migrate data across multiple regions for resiliency purposes, often a multi-region deployment is solely dependent on the CSC configuration.

### Disaster Recovery

An unidentified single point of failure and/or inadequate planning to address disaster recovery scenarios could result in a significant impact.

The BC/DR parameters are associated with solution design. A more resilient design often utilizes multiple components in different CSP availability zones and involve data replication.

| | | |
|---|---|---|
| As going to the cloud should make it quicker to come back online, the recoverability time depends on the SLA for the CSP. So, you should understand CSP service level agreements (SLAs) | Since recoverability is different in the cloud, CSC should provide documentation of agile processes and diagrams. | While the CSP provides service level agreements (SLAs) at the individual instance/service level, these should not be confused with a CSC's business continuity (BC) and disaster recovery (DR) objectives, such as: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). |

## Recap

- BCP are organizational safeguards and mechanisms that ensure the ongoing availability of information system functionality and access to data.
- Appropriate deployment, and assessment of this audit, it is critical that recommended multi-region with multi-availability zones are used.
- While a CSP may migrate data across availability zones for resiliency purposes, often a multi-region deployment is solely dependent on the CSC configuration.

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/c8285105-2e74-426d-95c2-a8af221012f3/AWS_CloudAuditAuditConsiderations.pdf