Cloud Audit Academy

Audit Considerations

Use this collection of considerations to help you start an audit plan.

Cloud Services & Scoping	
☐	1. Perform a walk-through of the services with the CISO, head of cloud, or security audit team to understand the documented process for whitelisting and approving cloud services a. Obtain list of services and validate if approval was in line with formal process.
☐	2. Review the service map and inventory. Ensure all the services that are listed in the inventory are also in the service map.
☐	3. Ensure all services you would expect to see for CSC workloads are being used.
☐	4. Ensure the services the CSC is consuming are included in the CSP's third-party attestation. Only services that are actually being used by the CSC should be in scope for the CSC audit.
☐	5. Ensure the CSC is using services that are compliant with the framework that is being assessed against. Note: 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, a CSC's additional security controls and design factors can result in the service's compliance. Sometimes the CSC will use risk acceptance based on concrete risk analysis to use the service.
☐	6. Obtain the inventory of the CSC's cloud systems, along with the network diagrams. a. Identify assets. Each cloud account has a contact email address associated with it and can be used to identify account owners. It is important to understand that this e-mail address may be from a public e-mail service provider, depending on what the user specified when registering, which is risky and can have serious repercussions. Note: The account owner may be someone in the finance or procurement department, but the individual who implements the organization's use of the CSP resources may reside in the IT department. You may need to interview both.
☐	7. Verify the CSC's cloud network is documented and all cloud critical systems are included in the inventory documentation (for their portion of the shared responsibility model). a. Ensure that resources are appropriately tagged and associated with application data. b. Review application architecture to identify data flows, planned connectivity between application components and resources that contain data.

Cloud Services & Scoping	
☐	8. Review all connectivity between the network and the cloud platform by reviewing the following: VPN connections where the on-premises public IPs are mapped to CSC's gateways in any private cloud owned by the CSC.

Governance, Risk, & Personnel	
☐	1. Understand the CSC's cloud governance strategy (governance tools, structure, monitoring, and reporting) a. Are they utilizing GRC tools? How are they leveraged? Do they work well with the CSP?
☐	2. For personnel, ensure the CSC trains their employees on cloud security best practices, verifying security awareness training records. a. Review the organizational structure to identify cloud appropriate roles (e.g. Chief Digital Officer (CDO)). b. Identify who owns and manages the CSP relationship, ensuring that is an appropriate person. c. Do the employees who make decisions about the cloud services have the education and skills to do so?
☐	3. Ask for a copy of the third party attestation and certifications in order to gain reasonable assurance of the design and operating effectiveness of control objectives and controls
☐	4. Ask for risk assessment documentation and examine if they reflect the current environment and accurately describe the residual risk environment. a. Is their cloud usage covered in their risk documentation?
☐	5. Assess and map third-party attestation to relevant risks to the CSC. The mapping will drive what needs to be audited at the CSP level versus the CSC. Look for the complementary user entity controls (CUEC). Ask the CSC to provide their response to each of the risks that the CSP states resides with the CSC.
☐	6. Identify key controls using the technology the CSP provides in their services. a. Understand who the admins and builders are. Who or what are the admins? Who has access to code? Are they the same people? In the cloud, admins can be services, system calls, roles, etc. b. Confirm the CSC has assigned an employee(s) as authority for the use and security of cloud services and there are defined roles for those noted as key roles, including a Chief Information Security Officer (CISO). c. Sample question: Ask about any published cybersecurity risk management process standards the CSC has used to model information security architecture and processes.
☐	7. Look at the CSC's internal controls for financial reporting. Does the contract include either a relevant attestation report and/or right-to-audit?
☐	8. Combine both the CSP attestation and your audit of the CSC's environment to perform a final gap-analysis a. Review the controls to ensure each control is covered either by the CSP, your audit or both.

Governance, Risk, & Personnel	
	b. Assess the control matrix holistically to ensure each control is covered.

Access Management	
☐	1. Ensure there are internal policies and procedures for managing access to CSP services and compute instances. a. Obtain a list of users with cloud access, validate their privileges are in line with their role. b. Obtain the cloud password/certificate/tokens policies, validate through a sample of users that they are compliant (check if there is a way to continuously monitor this) or ideally, federated to existing systems. c. Validate that access to the cloud is approved by appropriate personnel. d. Verify that periodic review of cloud users is preformed accurately and completely (e.g. is access updated when employees move between roles or outside of the CSC). e. Ensure documentation of use and configuration of CSP access controls, examples and options are outlined below:
☐	2. Ensure there is an approval process, logging process, or controls to prevent unauthorized remote access. a. Validate logs are complete and accurate. What is in place to demonstrate the logs are complete and accurate? If they do not have proof, you can validate by same testing to see if logs produce expected results. b. Review process for preventing unauthorized access. c. Review connectivity between firm network and CSP.
☐	3. Ensure restriction of users to those CSP services strictly for their business function. Review the type of access control in place as it relates to CSP services. a. CSP access control at a CSP level – using IAM with Tagging to control management of compute instances (start/stop/terminate) within networks. b. CSC Access Control – using access management (LDAP solution) to manage access to resources which exist in networks at the Operating System /Application layers. c. Ensure segregation of duties is documented and followed. d. Network Access control – using CSP virtual firewalls, Network Access Control Lists (NACLs), Routing Tables, VPN Connections, private cloud peering to control network access to resources within CSC owned private cloud. e. Access to edit/view/delta data – although not administering security, sensitive information still needs privileged access. f. Ensure the CSP region that hosts resources for CSC data has region-specific certifications.
☐	4. How does the CSC federate identity to the cloud? Is active directory the single source of code? Do they have multi- factor authentication on the root account? Who has the ability to create/delete accounts?

Access Management	
☐	5. Review the access management system (which may be used to allow authenticated access to the applications hosted on top of cloud services) and validate whether it is federated with the cloud systems.

Data Security	
☐	1. Understand what data the CSC has in the cloud and where the data resides, and validate the methods used to protect the data at rest and in transit (also referred to as "data in-flight" or "in motion"). a. Ask if the CSC has asked their CSP for evidence that their data doesn't go where it's not supposed to. Is it part of the contractual obligation? b. Determine what's in scope regarding regions and legislation. What CSP regions are being used? What regional/global legislation should be considered?
☐	2. Understand and verify the CSC approach to data protection: a. Data policies, data communication, and procedures in the cloud? How are they enforcing it? b. Data sanitization process, Data transmission footprint and sovereignty rules c. System and information integrity policy and procedure d. Flaw remediation, Malicious code protection, Information System monitoring e. Security alerts, advisories, and directives, Security function verification f. Software, firmware, and information integrity, Information input validation g. Memory protection, Review regional considerations h. Multi-region backups, fault tolerant zones, failover zones
☐	3. Understand if CSC is leveraging the existing mechanisms for encryption or building on-top-of the CSPs. a. Ensure there are appropriate encryption controls in place to protect confidential information (or highly sensitive) in transit and at rest while using CSP services. b. How is data shared in the cloud? Cloud access security broker (CASB)?
☐	4. Assess if the CSP services are compliant to the framework being assessed. If they are not, is it documented in the CSC's risk management documentation? Does the CSC have additional controls in place covering the service thereby making it compliant?
☐	5. Review methods for connection to CSP console.
☐	6. Review management API, storage, and databases for enforcement of encryption.
☐	7. Review internal policies and procedures for key management, including CSP services and compute instances.
☐	8. Review the controls the CSC has in place to manage shadow IT (hardware, software, applications being used without the knowledge of virtual firewalls).

Data Security	
☐	9. Review the procedure for conducting a specialized wipe prior to deleting the volume for compliance with established requirements. This is to ensure deletion of CSC data.

Network	
☐	1. Understand the CSP security requirements and what the CSP requires of each of their customers. a. Are the configurations that are managed by the CSC appropriate for their service usage?
☐	2. Understand how a packet traverses from node to node along the CSP and within the CSC environment
☐	3. Understand the connectivity with the cloud and if that traffic is encrypted. What can connect? User devices? VPN? Direct network connections? Are the connections appropriate? Are their limiting security rules to scope connectivity down to the minimum required? Who has access to configure and change VPN settings?
☐	4. Review CSP virtual firewalls implementation, CSP direct connection and VPN configuration for proper implementation of network segmentation and firewall setting for CSP services.
☐	5. Verify they have a procedure for granting remote, Internet or VPN access to employees for CSP Console access as well as remote access to networks and systems. a. Ask for evidence that there is only one way to provision access and that it hasn't changed over time.
☐	6. Review the DDoS layered defense solution running which operates directly on CSP reviewing components which are leveraged as part of a DDoS solution. How did the CSC think about DDoS protection? Did they protect main network traffic routes, or did they cover all possible routes to the virtual network? Can their virtual network resources scale in the event of increased network traffic load?

User Device Management	
☐	1. Understand the CSC's cloud network constructs and security boundaries.
☐	2. Ask for workflow diagrams between user device and the network construct.
☐	3. Review a copy of the mobile device management policy (MDM). Does the MDM allow for employees to bring their own device (BYOD)? If so, a. What are the policies and requirements? b. Do you have a management profiles on user mobile devices? c. How are user devices managed? d. How are they handling operating system updates?

User Device Management	
☐	4. Is there a cloud access security broker (CASB) in place? If so, a. Who is managing the policies and threat analytics? Does the CSP offer this as a service or is it a third- party?
☐	5. Understand the hand-off between CSP and the CSC. What is in the contract agreement? CSP SLAs?

Configuration Management	
☐	1. Validate that the operating systems and applications are designed, configured, patched and hardened in accordance with CSC policies, procedures, and standards. All OS and application management practices can be common between on-premises and cloud systems and services.
☐	2. Consider the inventory of relevant configurations. How has management determined configuration changes relevant to their environment?
☐	3. What changes are the responsibilities of the CSC versus the CSP? For example, a CSC may be responsible for change request, UAT, change deployment whereas the CSP could be responsible for development and integration testing.
☐	4. For changes that the CSC is responsible for, is there sufficient change management controls in place to ensure that management expectations are met and risks are addressed?
☐	5. Review documented process for configuration of cloud compute instances: Machine Images, Operating systems, Applications a. Are CSP-pushed configuration updates being reviewed?
☐	6. Understand the release schedules. Do the changes match the release schedules?
☐	7. Review API calls for in scope services for delete calls to ensure IT assets have been properly disposed.

Vulnerability Management	
☐	1. Determine the relevant risks to the environment. Understand what the CSC's cloud is used for, for e.g. storage or financial transactions.
☐	2. Identify what vulnerability scanning tools the CSC uses for their cloud services, either from their CSP, a third-party, or both.
☐	3. Check if scanning tools are being used, how tools are being used, and if the tools and its outputs are reliable.

Vulnerability Management	
☐	4. Review the output. a. Determine if the output match the compliance requirements. b. Understand what the CSC is doing with the output. c. Understand if the output is reviewed by management. d. Understand if the output addressing relevant risk(s).
☐	5. Review lessons learned and ensure the CSC has addressed any findings in a timely manner.
☐	6. Understand the CSC's approach to patching. Understand if the CSC is automatically accepting CSP forced patches or manually accepting them.
☐	7. Ask how the CSC is hardening their images and keeping them up-to-date, as the CSP is not responsible for it.
☐	8. Ask for documentation on how the CSC prioritizes and ranks vulnerabilities and SLAs. a. Moved where the environment exists? It could be in scope now when it wasn't before. b. Understand what protections (tools, technology, SLAs) the CSC has in place and how they are testing those since those are different now that the CSC is in the cloud. c. Understand how the CSC categorizes these protections.
☐	9. Ask how the CSC manages penetration testing, as it requires working with the CSP. Understand if they are doing it or not doing it because of the extra notification and coordination overhead.
☐	10. Assess what their vulnerability management looks like in their cloud environment. Understand if the controls are actually remediating the risk. Some best practices that should be present: a. Patch management strategy – controlling how info comes into the environment b. Proactive detection – pen testing c. Virus detection d. Border definition
☐	11. Confirm penetration testing has been completed.
☐	12. Verify cloud services are included within an internal patch management process.
☐	13. Assess the implementation and management of antimalware for compute instances in a similar manner as with physical systems

Monitoring and Logging	
☐	1. Understand the hand-off of ownership and responsibility in terms of what the CSP is responsible for versus the CSC.
☐	2. Understand all the risks so that the CSC can look for the logs that can alert to these risks.
☐	3. Understand the monitoring and logging tools the CSC is using that are provided by their CSP. Understand what functionality is turned on/off in those tools.

Monitoring and Logging	
☐	4. Ensure the CSC can access the logs as needed. a. Understand how the logs are being provided and where they are stored. b. Ensure the logs are consumable. c. Understand who has access to the logs and what level of access and permissions are configured d. Ensure the logs are protected and can be accessed only by approved and authorized personnel. e. Review the Access Management Credential report for unauthorized users and resource tagging for unauthorized devices. f. Understand if there are additional tools being used to supplement the CSP out-of-the-box logs. g. Confirm aggregation and correlation of event data from multiple sources.
☐	5. Understand how the CSC is using the CSP provided logs a. Understand ways the CSC is analyzing these logs that is different from the on-premises environment (if present). b. Understand the input logs and ensure they are being consumed into the security incident manager. c. Verify that logging mechanisms are configured to send logs to a centralized server, and ensure that for compute instances the proper type and format of logs are retained in a similar manner as with physical systems.
☐	6. Ensure CSC's employees have the right skills and knowledge to configure the logs correctly, and analyze and act on them.
☐	7. Identify applicable compliance requirements and review third-party attestation report to ensure those requirements are covered. a. Understand the relevant types of instances the CSC cares about that show up. b. To ensure completeness and accuracy, test the relevant transaction types by recreating instances to prove that the instances will actually show in the logs.
☐	8. Ensure the logs comply with policy. a. Review logging and monitoring policies and procedures for adequacy, retention, defined thresholds and secure maintenance, specifically for detecting unauthorized activity for cloud services. b. Validate that audit logging is being performed on the guest OS and critical applications installed on compute instances and that implementation is in alignment with CSC policies and procedures, especially as it relates to the storage, protection, and analysis of the logs. c. Ensure analytics of events are utilized to improve defensive measures and policies.
☐	9. Ensure the logs inform incident response. a. Review host-based IDS on the compute instances in a similar manner as with physical systems. b. Review evidence on where information on intrusion detection processes can be reviewed

Incident Response	
☐	1. Verify an Incident Response Plan exists. a. Understand the relevant risks exist and whether these risks considered as part of the plan. b. Ensure the plan has clear identification of the CSC versus CSP responsibilities. Understand if a RACI documentation is available within the plan. c. Ensure the plan outlines a communication path between the CSC and CSP. d. Verify that the Incident Response Plan undergoes a periodic review and changes related to CSP are made, as needed. e. Note if the Incident Response Plan has notification procedures and how the CSC addresses responsibility for losses associated with attacks or impacting instructions. f. Ensure the CSC's RTO and RPO are reflected in the incident response plan.
☐	2. Ensure the CSC is leveraging existing incident monitoring tools, as well as CSP available tools to monitor the use of CSP services.
☐	3. Understand the CSC's definition of an incident that impacts the risk of what's in the cloud. Ask for the definition of the communication escalation path. It can be the same as on-premises but understanding the hand-offs is important because the technology can be different in the cloud. Evaluate the process for incident closure/resolution.
☐	4. Understand what is in the CSP SLA for the following: a. Understand when a CSP is required to contact a CSC and when the CSC is required to contact their CSP. b. Understand how incidents are identified. Ensure the right level of precision/prioritization is being applied to communicate the right incidents. c. Understand the responsibility to mitigate a breach, the level of detail provided, and mechanisms in place that can be leveraged to monitor and evaluate a breach.
☐	5. Understand if the CSP reported any incidents to them.
☐	6. Understand the mechanism by which the CSC is confident in the accurateness and completeness of the reporting coming from the CSP. Example questions: a. How are you comfortable that you are being informed of all those incidents? b. How confident are you? c. Best practice answer: Those outputs are covered in previous attestation(s), and listed by name.
☐	7. Identify active point of contacts at both the CSP and CSC.

Business Continuity and Contingency Planning	
☐	1. Understand the impact of their cloud services to revenue, life, or death. Understand how each service impacts business operations and what the impact would be if it were to cease unexpectedly.

Business Continuity and Contingency Planning	
☐	2. Understand the importance of the cloud to their business continuity and ensure the CSC reconfirmed this solution and answer every year, as service consumption's change.
☐	3. Understand the disaster recovery and determine the fault-tolerant architecture employed for those critical assets.
☐	4. Ask for the BCP, including the CSP services utilized, and ensure it addresses mitigation of the effects of and recovery from a cybersecurity incident. a. Ensure that the RPO and RTO in the plan are in line with the business criticality. b. Ensure that CSP is included in the emergency preparedness and crisis management elements, senior manager oversight responsibilities, and the testing plan.
☐	5. Understand how the CSC is using the cloud for recoverability focusing on their use (for e.g. hot site), classification of recoverability times, testing the recoverability by falling back to the cloud.
☐	6. Look at contingency planning policies, procedures, alternate storage and processing, backup, recovery and reconstitution. Distinguish between data loss and continued operations. The different risks are determined for different sets. Specifically, for SaaS, which tend to be more volatile, understand how the CSC has prepared for a scenario where the SaaS provider shuts down.
☐	7. Ensure Business Continuity Plan has been tested.
☐	8. Review the CSC's periodic test of their backup system for CSP services. The cloud gives you the ability to do snapshots easier, ask how long the CSC is storing them. Are they encrypted?
☐	9. Review inventory of data backed up to CSP services as off-site backup.