Date: 22-10-2019

Audit Considerations

Introduction to the Cloud

1. There are two functions of auditing cloud environments. (1) Security in the cloud: These are the audit clients building on top of the cloud, and consuming cloud service provider (CSP) services. (2) Security of the cloud: Auditing cloud service providers, their individual services, and offerings like infrastructure and platforms as services. For the purposes of this training, you will be learning about auditing security in the cloud.

2. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc. For security auditing, you will assess the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

3. Understand where the delineation is between the security posture of the cloud provider and the audit client you are assessing.

4. Understand how you can request and evaluate third-party attestations and certifications in order to gain reasonable assurance of the design and operating effectiveness of control objectives and controls.

5. Assess and map third-party attestation to relevant risks to the audit client. The mapping will drive what needs to be audited at the CSP level versus the audit client.

6. Review the CSP provided evidence from its auditors for details on where information on intrusion detection processes can be reviewed that are managed by CSP for physical security controls. Words to do with physical security, such as “cabling” are an indication that the control sits with the CSP and you can verify it through their continuous audit documentation.

7. Combine the existing documentation with your analysis of the construct of the applications, operating systems and supporting software, and platform on the cloud to build a comprehensive audit of the environment.

8. Ask for a copy of the SOC report. Look for the complementary user entity controls (CUEC). Ask the client to provide their response to each of the risks that the CSP states resides with the client.

Services

1. Perform a walk through of the services with the head of cloud to understand how cloud services are whitelisted and approved. (a) Is there a documented process in place for whitelisting and approving services? (b) Obtain list of services and validate if approval was in line with formal process.

2. Ensure the services the audit client is consuming are included in the CSP's third-party auditor report or attestation. Only services that are actually being used should be in scope.

3. Review the service map/inventory. Are all the services listed in the inventory in the service map? Are all the services you would expect to see for their workloads being used?

4. Ensure the audit client is using services that are compliant with the framework that is being assessed against.

Governance & Risk

1. Understand the client's cloud migration plan. (a) Are all of the providers compliant with the regulations that you are subject to? If not, how is it documented in the risk management program and accepted? (b) Is their SOC report provided by a certified, approved firm? (c) Where are the CSP's regions? Are they in regions where the client cannot do business? This doesn't necessarily prevent the client from doing business with the CSP, you just need to be sure the client is routing traffic and workloads in appropriate regions for their business. (d) Who can commit the client to CSP services?

2. Understand the client's cloud governance strategy. (a) What governance structure is in place? Is it formalized? How is it monitored? What reporting hierarchy do you follow? (b) Is their cloud usage covered in their risk documentation? (c) Are they utilizing GRC tools? How are they leveraged? Do they work well with the CSP? (d) Do the employees who make decisions about the cloud services have the education and skills to do so?
For personnel, ensure the client trains their employees on cloud security best practices, verifying security awareness training records. Review the organizational structure to identify cloud appropriate roles (e.g. Chief Digital Officer (CDO)). Identify who owns and manages the CSP relationship, ensuring that is an appropriate person.
How do they monitor/govern their cloud relationships? For example, if there is a use of cloud application services, do they have a steering committee that evaluates changes/patch releases prior to ingesting into the environment?

3. Obtain the inventory of the client's cloud systems, along with the network diagrams. (a) IIdentify 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. (b) Verify the client's cloud network is documented and all cloud critical systems are included in the inventory documentation (for their portion of the shared responsibility model).
Ensure that resources are appropriately tagged and associated with application data. Review application architecture to identify data flows, planned connectivity between application components and resources that contain data. (c) 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 audit client's gateways in any VPCs owned by the client.

4. Identify key controls using the technology the CSP provides in their services. (a) Identify what incremental controls are necessary to address based on the mapping of the third-party attestation to the audit client's relevant risks. Are there any complementary user entity controls that need to be considered? (b) 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. (c) Confirm the client 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). Sample question: Ask about any published cybersecurity risk management process standards the client has used to model information security architecture and processes.

5. Ask for risk assessment documentation. Examine if they reflect the current environment and accurately describe the residual risk environment.

6. Combine both the CSP attestation and your audit of the client'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. (b) Assess the control matrix holistically to ensure each control is covered.

7. Look at their internal controls over financial reporting. Does the contract include either a relevant attestation report and/or right-to-audit?

Identity & Access Management

1. Ensure there are internal policies and procedures for managing access to CSP services and compute instances. (a) a. Obtain a list of users with cloud access, validate their privileges are in line with their role. (b) 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) c. Validate that access to the cloud is approved by appropriate personnel. (d) 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 client). (e) e. Ensure documentation of use and configuration of CSP access controls, examples and options are outlined in the course.

2. Ensure there is an approval process, logging process, or controls to prevent unauthorized remote access. (a) 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) b. Review process for preventing unauthorized access. (c) c. Review connectivity between firm network and CSP.

3. Ensure restriction of users to those CSP services strictly for their business function. (a) a. Review the type of access control in place as it relates to CSP services.

Data Security & Privacy

1. Understand what privacy regulations are important to the client. Is their CSP compliant?

2. Understand what data the client 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 client 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?

3. Understand if audit client is leveraging the existing mechanisms for encryption or building on-top-of the CSPs.

4. Assess if the individual CSP services are compliant to the framework you are assessing. If they are not, is it documented in the client’s risk management documentation? Are additional controls the client has in place that cover the service thereby making it compliant for the client’s own purposes?

5. Ensure there are appropriate encryption controls in place to protect confidential information (or highly sensitive) in transit and at rest while using CSP services. How is data shared in the cloud? Via trusted entity? Cloud access security broker?

6. Review methods for connection to CSP console.

7. Review management API, storage, and databases for enforcement of encryption.

8. Review internal policies and procedures for key management including CSP services and compute instances.

9. Review encryption methods used, if any, to protect PINs at rest.

10. Check algorithms and key lengths.

11. Understand and verify the client approach to data protection.

12. Controls to manage shadow IT.

Network Management

1. Understand the CSP security requirements and what the CSP requires of each customer. Are the configurations managed by the customer appropriate for their service usage?

2.Understand how a packet traverses from node to node along the CSP backbone and within the client environment.

3. Understand the connectivity with the cloud. What can connect? User devices? VPN?

4. Review CSP Security Group implementation, CSP direct connection and VPN configuration for proper implementation of network segmentation and ACL and firewall setting or CSP services.

5. Verify they have a procedure for granting remote, Internet or VPN access to employees for CSP Console access and 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 following to maintain an environment for testing and development of software and applications that is separate from its business environment.

7. Review DDoS layered defense solution running which operates directly on CSP reviewing components which are leveraged as part of a DDoS solution.

8. Assess the implementation and management of antimalware for compute instances in a similar manner as with physical systems.

User Device Management

1. Understand the client's cloud network constructs.

2. Ask for workflow diagrams between user device and the network construct.

3. Ask to review a copy of the mobile device management policy (MDM).

4. Does the MDM allow for employees to bring your 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 OS updates?

5. Is there a cloud access security broker (CASB) in place? If so, (a) Who Is managing the policies, DOP, and threat analytics? (b) Does the CSP offer this as a service or is it a third-party?

6. Understand the hand off between CSP and the client. 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 audit client policies, procedures, and standards. All OS and application management practices can be common between on-premises and cloud systems and services.

2. Validate that the operating systems and applications are designed, configured, patched and hardened in accordance with audit client policies, procedures, and standards. All OS and application management practices can be common between on-premises and cloud systems and services.

3. Review the procedure for conducting a specialized wipe procedure prior to deleting the volume for compliance with established requirements.

4. Review your Identity 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.

5. Confirm penetration testing has been completed.

6. What kinds of changes are available to the audit client?

7. What changes are the responsibilities of the audit client versus the CSP? For example, an audit client may be responsible for change request, UAT, change deployment whereas the CSP could be responsible for development and integration testing.

8. For changes that the audit client is responsible for, is there sufficient change management controls in place to ensure that management expectations are met and risks are addressed?

9. For those areas that are the responsibility of the CSP, are they covered by an attestation report?

10. Verify cloud services are included within an internal patch management process. Review documented process for configuration and patching of cloud compute instances: (a) Machine Images, Operating systems, Applications

11. Understand the release schedules. Do the changes match the release schedules?

12. Ensure the audit client minimizes impact to controls by CSP-pushed patches. Are CSP-pushed patches and configuration updates being reviewed?

13. 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 audit client's cloud is used for, for e.g. storage or financial transactions.

2. Identify what vulnerability scanning tools the audit client uses for their cloud services, either from their CSP, a third-party, or both.

3. Check if scanning tools are being used, how the tools are being used, and if the tools and its outputs are reliable.

4. Review the output. (a) Determine if the output match the regulatory requirements. (b) Understand what the client 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 client has addressed any findings in a timely manner.

6. Understand the client's approach to patching. (a) Understand if the client is automatically accepting CSP forced patches or manually accepting them.

7. Ask how the client 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 client prioritizes and ranks vulnerabilities and SLAs. (a) Moved where the environment exists? Note: It could be in scope now when it wasn't before. (b) Understand what protections (tools, technology, SLAs) the client has in place and how they are testing those since those are different now that the client is in the cloud. (c) Understand how the client categorizes these protections.

9. Ask how the client manages penetration testing, as it requires working with the CSP. (a) 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 information comes into the environment (b) Proactive detection - penetration testing (c) Virus detection (d) Border definition

Monitoring & Logging

1. Understand the hand off of ownership and responsibility in terms of what the CSP is responsible for versus the client.

2. Understand all the risks so that you can look for the logs that can alert to these risks.

3. Understand the monitoring and logging tools the client is using that are provided by their CSP.

4. Ensure the client can access the logs as needed. (a) Understand how the logs are being provided and where is 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 IAM 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 client is using the CSP provided logs
. (a) Understand ways the client 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 client's employees have the right skills and knowledge to configure the logs correctly, and analyze and act on them.

7. Ensure the audit log is covered in the SOC report. (a) Understand the relevant types of instances the client 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 client 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 audit client versus CSP responsibilities. Understand if a RACI documentation is available within the plan. (c) Ensure the plan outlines a communication path between the audit client 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 audit client addresses responsibility for losses associated with attacks or impacting instructions. (f) Ensure the audit client’s RTO and RPO are reflected in the incident response plan.

2. Ensure the client is leveraging existing incident monitoring tools, as well as CSP available tools to monitor the use of CSP services.

3. Understand the client’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 handoffs is important because the technology can be different in the cloud.

4. Understand what is in the CSP SLA. the following: (a) Understand when a CSP is required to contact a client and when a client is required to contact their client? (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 client’s CSP reported any incidents to them.

6. Understand the mechanism by which the audit client 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 the SOC report, and listed by name.

7. Identify active point of contacts.

Business Continuity & Contingency Planning

1. Understand the impact of their cloud services to revenue, life, or death.

2. Understand the importance of the cloud to their business continuity and ensure the client 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. Also ensure BCP has been tested. (a) Ensure that the RPO and RTO in the plan are in line with the business criticality. (b) Within the Plan, ensure that CSP is included in the emergency preparedness and crisis management elements, senior manager oversight responsibilities.

5. Remember: The BCP is not the same thing as system recoverability.
   Understand how the client 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. Note: As going to the cloud should make it quicker to come back online, the recoverability time depends on the SLA for the CSP. Since recoverability is different in the cloud, client should provide documentation of agile processes and diagrams.

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 client has prepared for a scenario where the SaaS provider shuts down.

7. If the audit focus is on compliance with privacy standards or PHI, ensure that the client has thought about hardening the back-up solution so it is compliant. This needs to be assessed frequently as the client business changes, for e.g. if the client buys another company and their e-commerce footprint changes, the client needs to plan for how that acquisition affects the BCP and where and how the hand offs between them and their CSP occur.

8. Ensure BCP has been tested.

9. Review the audit client’s periodic test of their backup system for CSP services. The cloud gives you the ability to do snapshots easier, ask how long the client is storing them. Are they encrypted?

10. Review inventory of data backed up to CSP services as off-site backup.