Vendor Risk Assessment (Part -3)

Cloud Security Audit

S.No.	Area Covered
1	System Access requirements
2	Data Security & Integrity
3	Audits, Compliance & Risk Governance
4	Business Continuity
5	Change Management
6	Data Center Security
7	Key Management
8	Incident Management
9	Others
10	System Availability
11	Data Security
12	System & Network Security
13	Application and Data Security

SACHIN HISSARIA
CA | CISA | DISA | CEH | COBIT-19 | ISO27001:2022 | RPA | CC-ISC 2 | Trainer

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
System Availability	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	Medium			
Data Security	Do you provide a capability to identify virtual machines/hardware via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Medium			
Data Security	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Medium			
Data Security	Is automated equipment identification such as NAC used as a method to validate connection authentication integrity based on known equipment location?	High			
Data Security	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	High			
Data Security	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	High			
Data Security	Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	High			
Data Security	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?	Medium			
Data Security	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	High			
Data Security	Do you regularly review for appropriateness of the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	High			
Data Security	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g.., OVF) to help ensure interoperability?	High			
Data Security	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	Medium			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security	Are the System logs generated and stored in a secure tamper-resistant environment? Do you have NTP Server implemented? NTP servers should be deployed to imprint correct timestamps which would further assist in co-relation. Furthermore, NTP systems should be periodically checked for time-drifts.	High			
Data Security	Are the appropriate rules defined such that only necessary ports are accessible for intranet / external network / corporate network / administrative access?	High			
Data Security	Does all management interfaces in the PaaS environment secured with strong passwords (authentication) & authorizations?	High			
Data Security	Does all management interfaces in the container environment only accessible to management IP addresses/VLANs?	High			
Data Security	Are all patches installed as per the client's patching policy (usually n-1) for the host OS, Virtualization environment, third-party software's?	High			
Data Security	Are all critical patches installed on host OS, VM environment, third-party software's as soon as their advisories are released?	High			
Data Security	Are the critical systems which don't require public access over the internet access-controlled by appropriate network rules, VLANs, etc.?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security	Do Containers allow users to deploy their applications in a safe and secure way, knowing that one application cannot interact with any other on the PaaS unless it is specifically allowed to?	High			
System & Network Security	Are the adequate controls deployed to monitor system performance and resource utilization during both peak & non-peak hours?	High			
Data Security	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	High			
Data Security	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Low			
Data Security	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	High			
Data Security	Do you allow tenants to use third-party identity assurance services?	Medium			
Data Security	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Medium			
Data Center Security	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Center Security	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	Medium			
Data Center Security	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	Medium			
Data Center Security	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Medium			
Data Center Security	Do you provide redundancy and availability for data center as per Industry Standard?	Medium			
Data Centre Security	Is the Datacenter certified?	High			
Key Management	Do you have key management policies binding keys to identifiable owners?	High			
Key Management	Do you have a capability to allow creation of unique encryption keys per tenant?	High			
Key Management	Do you maintain key management procedures for separation of tenants?	Low			
Key Management	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Low			
Key Management	Do you encrypt tenant data at rest (on disk/storage) within your environment?	High			

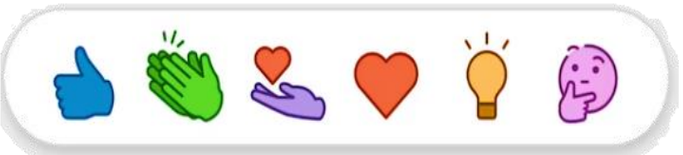
Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Key Management	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	High			
Key Management	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	Medium			
Key Management	Do you store encryption keys in the cloud?	High			
Incident Management	Do you have a documented security incident response plan?	Medium			
Incident Management	Do you integrate customized tenant requirements into your security incident response plans?	Medium			
Incident Management	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	Medium			
Incident Management	Have you tested your security incident response plans in the last year?	High			
Incident Management	Is access to any systems that contains tenant data logged?	High			
Incident Management	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Incident Management	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	High			
Incident Management	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	High			
Others	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Medium			
Others	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant systems?	Medium			
Others	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Medium			
Others	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Medium			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks

IF YOU FIND THIS USEFUL , SHARE WITH YOUR NETWORK.
FOLLOW FOR MORE SUCH CHECKLIST | TEMPLATE | IT AUDIT RELATED STUFF

@SACHIN_HISSARIA



YouTube https://youtube.com/@sachinhissaria6512