Vendor Risk Assessment (Part -1)

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 Access requirements	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	Medium			
System Access requirements	Are all requirements and trust levels for customers' access defined and documented?	Medium			
System Access requirements	Is there any wireless access network implemented at any data center? If yes, is it connecting with the network provided to tenants?	Low			
System Access requirements	Do you document how you grant and approve access to tenant data?	Medium			
System Access requirements	Do you provide, upon request, user access (e.g. employees, contractors, customers / tenants, business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Low			
System Access requirements	If users are found to have inappropriate access, are all remediation and certification actions recorded?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
System Access requirements	Will you share user access remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	Low			
System Access requirements	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	Low			
System Access requirements	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	Low			
System Access requirements	Does legal counsel review all third-party agreements?	Medium			
System Access requirements	Do you have a defined policy and procedure for User Lifecycle management?	Medium			
System Access requirements	Do third-party agreements include provision for the security and protection of information and assets?	Medium			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security & Integrity	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	High			
Data Security & Integrity	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	High			
Data Security & Integrity	Do you have capability to recover data for a specific customer in the case of a failure or data loss?	High			
Data Security & Integrity	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	High			
Data Security & Integrity	Do you produce audit assertions using a structured, industry accepted format (e.g., Cloud Audit/A6 URI Ontology, Cloud Trust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Medium			
Data Security & Integrity	Do you have a capability to use system geographic location as an authentication factor for administrative activities?	Medium			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security & Integrity	Can you provide the physical location/geography of storage of a tenant's data upon request or in advance?	High			
Data Security & Integrity	Can you ensure that data does not migrate beyond a defined geographical residency?	High			
Data Security & Integrity	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	High			
Data Security & Integrity	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	High			
Data Security & Integrity	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	High			
Data Security & Integrity	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security & Integrity	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	Medium			
Data Security & Integrity	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	Medium			
Data Security & Integrity	Do you monitor and log privileged access (administrator level) to information security management systems?	Medium			
Data Security & Integrity	Do you use dedicated secure networks with multi-factor authentication to provide management access to your cloud service infrastructure?	High			
Data Security & Integrity	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	High			
Data Security & Integrity	Do you support the ability to force password changes upon first logon?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security & Integrity	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	Low			
Data Security & Integrity	Are file integrity (host), Data Leakage Prevention (DLP), Network Intrusion Detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	High			
Data Security & Integrity	Is physical and logical user access to audit logs restricted to authorized personnel?	High			
Data Security & Integrity	Are audit logs centrally stored and retained?	High			
Data Security & Integrity	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	High			
Data Security & Integrity	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Medium			

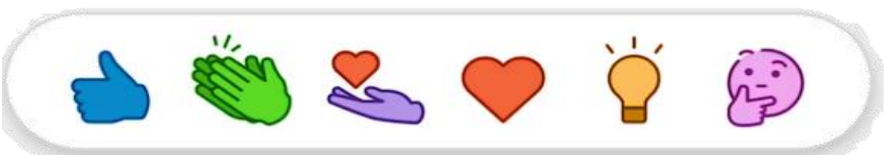
Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security & Integrity	Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	Medium			
Data Security & Integrity	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	High			
Data Security & Integrity	Are all firewall access control lists documented with business justification?	Medium			
Data Security & Integrity	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	High			
Data Security & Integrity	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	High			
Data Security & Integrity	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security & Integrity	Do you implement technical measures and apply defence-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	High			
Data Security & Integrity	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	High			
Data Security & Integrity	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	High			
Data Security & Integrity	Do you ensure that security threat detection systems using signatures, lists or behavioural patterns are updated across all infrastructure components within industry accepted time frames?	High			
Data Security & Integrity	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? What is the time taken to close the gaps and retest the same?	High			
Data Security & Integrity	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? What is the time taken to close the gaps and retest the same?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Data Security & Integrity	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	High			
Data Security & Integrity	How is disk media destroyed when decommissioned?	Low			
Data Security & Integrity	Is data backed up or copied?	High			

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

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks