Vendor Risk Assessment (Part -2)

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
Audits, Compliance & Risk Governance	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	High			
Audits, Compliance & Risk Governance	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, firewalls, operating systems, routers, DNS servers, etc.)?	Medium			
Audits, Compliance & Risk Governance	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	High			
Audits, Compliance & Risk Governance	Do you conduct risk assessments associated with data governance requirements at least once a year?	High			
Audits, Compliance & Risk Governance	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	High			
Audits, Compliance & Risk Governance	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	Medium			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Audits, Compliance & Risk Governance	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Medium			
Audits, Compliance & Risk Governance	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Medium			
Business Continuity	Do you provide tenants with infrastructure service failover capability to other providers?	Low			
Business Continuity	Are business continuity plans documented and subjected to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Medium			
Business Continuity	Do you provide tenants with documentation showing the transport route of their data between your systems?	Medium			
Business Continuity	Can tenants define how their data is transported and through which legal jurisdictions?	Medium			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Business Continuity	Does your cloud solution include provider independent restore and recovery capabilities?	Medium			
Business Continuity	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	High			
Business Continuity	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Low			
Business Continuity	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	High			
Business Continuity	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	Medium			
Business Continuity	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Business Continuity	Do you test your backup or redundancy mechanisms at least annually?	High			
Business Continuity	Do you provided a tenant-triggered failover option?	Medium			
Change Management	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	High			
Change Management	Is documentation available that describes the installation, configuration and use of products/services/features?	Medium			
Change Management	Is documentation describing known issues with certain products/services available?	Medium			
Change Management	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Change Management	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Medium			
Change Management	Do the employment change/termination procedures and guidelines account for timely revocation of access and return of assets?	High			
Change Management	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Medium			
Data Center Security	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	High			
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			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
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			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
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			
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			

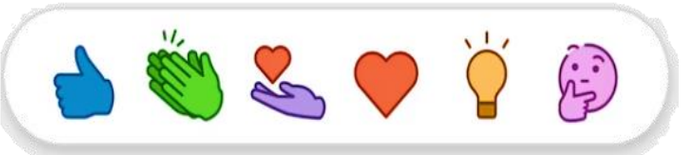
Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Incident Management	Do you integrate customized tenant requirements into your security incident response plans?	Medium			
Incident Management	Do you publish a roles and responsibilities document specifying what you 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			
Incident Management	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
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	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	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