Vendor Risk Assessment (Part -4)

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
Application and Data Security	Describe your application's architecture and different tiers	Low			
Application and Data Security	Do you follow industry standard coding practice?(If yes, verify the coding practice guideline.)	High			
Application and Data Security	What testing approach do you follow. (E.g. Agile/Staggered/other)	Low			
Application and Data Security	Do you perform web application vulnerability testing? What is the frequency?	High			
Application and Data Security	Are the API keys managed and stored securely?(Public access to the API keys should be prohibited.)	High			
Application and Data Security	Does SaaS application support identity federation standards (SAML, SPML, WS-Federation, MFA, OTP & Oauth)?	High			
Application and Data Security	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	High			
Application and Data Security	Do you verify that all of your software/software components suppliers (if any) adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Medium			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Application and Data Security	Do you review your applications for security vulnerabilities (E.g.: OWASP top-10) and address any issues prior to deployment to production?	High			
Application and Data Security	Is source code review performed by Cert-IN empanelled testing agency for applications?	High			
Application and Data Security	Do you use manual source-code analysis to detect security defects in code prior to production?	High			
Application and Data Security	Are all production, development, QA, testing environment segregated? Is the access to production systems allowed as per the business-requirement?	High			
Application and Data Security	Are the Data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	High			
Application and Data Security	Do you have encryption standard (e.g.: HTTPs) for secure transmission of data (Data in transit)?	High			
Application and Data Security	Are all sensitive data at rest encrypted using strong cryptographic standards such as AES-128 OR above?	High			
Application and Data Security	In a client-server application model, is the synchronization between the two encrypted using well known encryption algorithms?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Application and Data Security	Does the SaaS provider have access to client OR any customer related data?	High			
Application and 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			
Application and Data Security	Do you have controls in place to detect source code security defects for any outsourced software development activities?	High			
Application and Data Security	Do you provide your tenants with documentation that describes your quality assurance process?	Medium			
Application and Data Security	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	High			
Application and Data Security	Do you have a Policy Enforcement capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	High			
Application and Data Security	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	Medium			

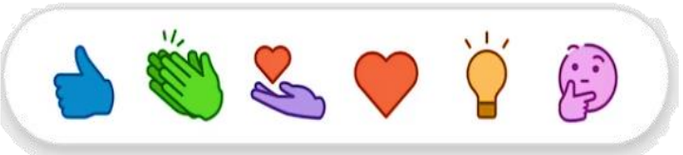
Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
Application and Data Security	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	High			
Application and Data Security	Do you provide tenants with separate environments for production and test processes?	High			
Application and Data Security	Is code authorized before its installation and use, and the code configuration checked, to ensure that the authorized code operates according to a clearly defined security policy?	High			
Application and Data Security	Is all unauthorized code prevented from executing?	High			
Application and Data Security	Do you protect user authentication information?	Medium			
Application and Data Security	How are User Files stored? What level of encryption?	High			
Application and Data Security	How is tenant account information for the application stored?	High			
Application and Data Security	Are User Files accessed by the vendor?	Medium			
Application and Data Security	Is the access to User File restricted?	High			
Application and Data Security	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	High			

Control	Control Activity	Risk Rating	Compliance Status	Vendor Remarks	Auditor Remarks
System & Network Security	Is the access to Production System restricted?	High			
System & Network Security	Is access to the system logged?	High			
System & Network Security	Do you perform vulnerability scans and penetration testing on Production environment?(Verify the latest VAPT Report)	High			
System & Network Security	What type of firewalls do you use?	Low			
System & Network Security	Is the system/network monitoring, logging and alerting setup in place?	High			
Others	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	High			
Others	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	High			

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