Third-Party Risk Assessment (TPRA) Checklist

Prepared By – Sachin Hissaria

in/sachin-hissaria

@sachinhissaria6512

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
1	Access Control	Is there a periodic user access review for the user profiles by the system administrator? Mention the details of the sample evidence.		
2	Access Control	Is there a mechanism that informs the security personnel of the lost access cards (if available) or termination of access rights to personnel involved in "Company name" scope of work?		
3	Access Control	Is there a well-defined process for removing the user account and access rights at the time of an employee leaving the vendor's processing facility?		
4	Access Control	Is there a provision for automatic lockout of accounts after a predefined number of unsuccessful attempts? If Yes, what is the count of the unsuccessful attempts after which the account lockout?		
5	Access Control	Is there a password policy defining the framework for a strong password? Does the system prompt the change of user passwords at predefined intervals? If Yes, what is the time line ? Check for: - Password Complexity - Password history - Maximum password age - Reversible encryption Check for sample user IDs without password.		
6	Access Control	Is a "secure password distribution mechanism " in place? Specify the mechanism, if applicable.		
7	Access Control	Is Password masked on the screen during the log-in process. Are the user access passwords displayed / stored / transmitted in clear text over the network?		
8	Access Control	Are following actions performed on all systems used for "Company name" operations- -Internet access on need basis -admin privileges restricted -Restricted email access -Disable access to printers -Access to printers -Is sharing of Local drives disabled across all the system?		
9	Access Control	Is Guest Account disabled ?		
10	Access Control	Are the end users provided with local admin rights? Are the access to command prompt restricted to have admin rights and registry editing disabled on all the desktop across the organization?		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
11	Access Control	Are the ports blocked for floppy/CD/DVD drives & USB Ports? Does the Vendor have any centralized mechanism in place to track the same? Mention the details of the mechanism.		
12	Access Control	What are the different levels of administrator privileges for system access on "Company name" specific servers? Are these access rights periodically reviewed ?		
13	Access Control	Are the network access points (Wi-Fi) at Vendor's premises available in public areas like reception, conference rooms etc.? Can unauthorized personnel connect to Wi-Fi network?		
14	Antivirus & Patch Management	Does the vendor have an Antivirus Signature Management System in place for systems related to the "Company name" operations? -Are the AV signatures are up to date? -Are records for the same maintained? -Specify the frequency defined for signature Updation.		
15	Antivirus & Patch Management	Is antivirus software deployed, updated and maintained for all desktops, servers, firewalls, and Internet email gateways? Describe what anti-virus products are used with each platform.		
16	Antivirus & Patch Management	Has the Anti-virus software been configured to log anti-virus activities, such as weekly scans, virus detection, and signature file updates?		
17	Antivirus & Patch Management	Has Anti-Virus software been configured for real-time scanning against all file write activity?		
18	Antivirus & Patch Management	Are controls in place to prevent end users from overriding or disabling the antivirus software?		
19	Antivirus & Patch Management	Do you have patch management policy? Is there a defined and documented process for implementing Security patches on systems for "Company name" operations? Are the roles & responsibilities are defined? Specify the frequency defined.		
20	Antivirus & Patch Management	Does the Vendor ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed?		
21	Antivirus & Patch Management	Are patches tested in a UAT instance before deployment on the production server ?		
22	Application Security	Is Appsec performed for internet facing applications used for "Company name" operations?		
23	Application Security	What is inactivity timeout period specified for the applications?		
24	Asset management	Is approved hard drive encryption software deployed on portable digital devices and systems (e.g. mobile phone, laptop, tablet etc.) that hold sensitive data? If yes, please specify the details of the solution being used for the same.		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
25	Asset Management	Is the movement of assets (used for "Company name" operations) tracked / monitored and reconciled at the Vendor facility ?		
26	Asset management	Is there a mechanism to ensure that only licensed software / applications are installed on the systems? Mention the details of the mechanism.		
27	Business continuity management	Is there an alternate/BCP location facility & supporting facility to continue "Company name" operations? Is testing done for movement of "Company name" operations from primary site to alternate site? Check the testing report		
28	Business continuity management	Does the organization have a documented IT DR plan addressing people, process & systems related to "Company name" operations? Is it communicated to concerned employees?		
29	Business continuity management	Can the backed up data be restored and made available at the alternate site at any point in time? Can the critical data be restored in the time frame as agreed with "Company name"?		
30	Business continuity management	Is there secondary network link available which can be used in case of failure of primary network link?		
31	Cloud Security	Does the vendor store, process, transmit "Company name" data over cloud from cloud service providers? Where is the data stored within India or overseas ? Please provide details.		
32	Data Security	Does the Vendor have a mechanism in place to classify & protect "Company name" related data. (Refer Information Classification Policy) E.g. Confidential/Restricted/Public Mention the details of the sample evidence.		
33	Data Security	Does the vendor have data leakage prevention capability? (if applicable, provide details)		
34	Data Security	Doe the vendor have a database level segregation for "Company name" critical (SPDI, PII and Card data) data?		
35	Data Security	1. Does the Vendor have a defined retention period for "Company name" data? 2. Does the Vendor have a process for secure removal / disposal / purging/ destruction of "Company name" data? 3. Is "Company name" notified after every deletion cycle. Mention the details of the sample evidence.		
36	Email Usage	Check the user e-mail ID creation process. Is there appropriate approvals from HR/ management for creating such email accounts at the vendor processing facility?		
37	Email Usage	Are e-mail /user ids created if the "Company name" related operations are outsourced / sub-contracted to other parties? If yes, Are proper approvals are taken for the same.		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
38	Email Usage	Does the Vendor have a provision of shared email account. Verify and mention if there is a mechanism in place to ensure accountability of shared email accounts, if any.		
39	Email Usage	Does the Vendor have a defined Data Leakage Prevention(DLP) mechanism in place to ensure that the "Company name" data is not sent via email to non-"Company name" IDs? Does the vendor has Mail Authentication System (Like DMARC) in place? (Based on applicability)		
40	Email Usage	Are the email attachments sent/received for the "Company name" process scanned for Virus and other malicious content?		
41	Email Usage	Is the customer data shared over email? Are the attachments sent to "Company name" being encrypted or password protected before sending?(at least 128 bits) Mention the details of the encryption mechanism, if applicable.		
42	Email Usage	Does the e-mail communication from the vendor include a standard disclaimer as a part of the contents. (Applicable in cases where vendor sends email on behalf of "Company name")		
43	Incident Management	Are roles & responsibilities defined for reporting suspected security incidents to "Company name"? Are the root cause analysis performed for the security incidents.		
44	Incident Management	Does the Vendor have a incident response plan in place to be implemented in the event of system breach. If yes, does the plan assess the following, at a minimum: - Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business continuity procedures - Data back-up processes - Analysis of legal requirements for reporting compromises - Coverage and responses of all critical system components - Reference or inclusion of incident response procedures from the payment brands		
45	Incident Management	Is there a repository / database for logging past Security Incidents ? Describe the mechanism to establish learning from past incidents?		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
46	Information Security Policy & Management	1. Do you have a documented and approved Information Security policy and procedures? 2. Is there an owner specified, who is responsible for maintaining the information security policy? Specify the date (Enter in comments column) on which management last approved the policy, if applicable.		
47	Information Security Policy & Management	Do you have an acceptable usage policy (for usage of corporate computing resources including restriction on using email, USB, Internet browsing)? Is it mandated to all the employees? Do you have Internet/Intranet access and Email usage policy?		
48	Information Security Policy & Management	Does the Vendor have a defined policy for data handling. Does the policy cover Data Privacy and Secure usage, storage and destruction of confidential data?		
49	Information Security Policy & Management	Do you have Key Management or Encryption / Decryption Policy?		
50	Information Security Policy & Management	Do you have Security incident management policy? Does the policy cover the following: - Security Incidents - Security Weakness - Software Malfunctions - Malicious Software		
51	Information Security Policy & Management	Do you have Access Control, Physical security policy and procedure? Does the policy cover the following(if applicable): -physical access, system/user access (role based access control & structured process for creation of new user account for "Company name" operations) -hardware, software, storage media, paper recorders, photo copiers, mail, fax, facilities(access control)		
52	Information Security Policy & Management	Do you have Disaster recovery and business continuity plan / policy covering people, process & system related to "Company name" operation?		
53	Information Security Policy & Management	Do you have an Asset Management Policy? Does the policy includes classification & protection of sensitive IT assets covering "Company name" activities/processes?		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
54	Information Security Policy & Management	Do you have a backup and recovery policy?(Covering "Company name" Operations) Does the Backup & Recovery Policy & Procedure document considers the following - - essential business information & software to be backed up? - servers to be backed up? - audit trail & logs? - frequency of backup? - Logging of Backup activity? - Retention period for backup? - Roles & responsibilities defined & assigned?		
55	Information Security Policy & Management	Do you have Anti-Malware/Anti-Virus Policy?		
56	Information Security Policy & Management	Are all the policies communicated to all the employees working for "Company name"? If yes, mention the method and frequency of communication?		
57	Information Security Policy & Management	1. Do you have a Risk Management Policy(Assets) ? 2. Mention the frequency defined for conducting regular Vulnerability & Risk Assessments.		
58	Information Security Policy & Management	What is the data retention and purging policy or procedure? Is it same or different for encrypted, decrypted and un-encrypted data?		
59	Information Security Policy & Management	Does the vendor have a comprehensive Mobile Device and Communications Policy covering use of Handheld devices, portable devices, mobiles, laptops, tablets etc. for Operations including "Company name".		
60	Miscellaneous Checks	Do you have repository of customer complaints reported to the bank?(if applicable)		
61	Miscellaneous Checks	Do you have appropriate mechanism to prevent & detect fraud ?		
62	Network Management	Does the vendor have a comprehensive network architecture diagram covering infrastructure used for "Company name" operations? Mention the details for the same.(E.g. Design approval details)		
63	Network Management	Are all internet facing servers placed in DMZ?		
64	Network Management	Are the inbound and outbound traffic restricted to that which is necessary for the "Company name" data environment?		
65	Network Management	Is the Documentation and business justification present for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.		
66	Network Management	Is the internet access or internet usage restricted and controlled? Mention the details for the same. (E.g. IP address)		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
67	Network Management	Is the firewall configured for the stateful inspection/dynamic packet filtering? (That is, only “established” connections are allowed into the network.)		
68	Network Management	Is VA / PT of network devices performed periodically? If yes, verify and specify the periodicity.		
69	Network Management	Is there a proactive mechanism to monitor unauthorized network access attempts?(Internal /external) External : Check if there IDS/IPS implemented in the environment ? If yes, ask for make and model of device. Mention the details for the same.		
70	Network Management	Has the vendor maintained redundancy for firewall & other network components? Mention the details of the redundant major devices, if applicable.		
71	Network Management	Are the modification in the firewall rule for "Company name" operations follow the change management process. Mention the details of the sample evidence.		
72	Network Management	What is the mechanism used for securing the connectivity between the Vendor and the "Company name". Mention the details for the same? E.g. Lease line connectivity (with data sent in encrypted form) or VPN.		
73	Network Management	Are the network devices and servers used for providing services to the "Company name" are physically and logically segregated?		
74	Network Management	Does the Vendor have a mechanism to identify and authenticate the user for external access (e.g., remote - VPN, wireless and third party) to the Vendor’s network. Mention the details of the mechanism and sample evidence.		
75	Network Management	Is there a defined process for installing & encrypting wireless access points, if any used by vendor?		
76	Network Management	Is "Company name" data segregated from other clients data on SFTP server or any where if stored ?		
77	Network Management	Is 2-factor authentication used for every critical applications.		
78	Network Management	Is the firewall rule base reviewed at regular intervals? If yes, verify and specify the periodicity.		
79	Operation Management	1. Do you have a documented procedure for identifying -the changes to be notified to the "Company name", -approval for the same, and - communication process , if needed? 2. Is there an established SPOC for notifying these changes to the "Company name" and maintaining the documentation for the same?		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
80	Operation Management	Is there a change management process, for activities of "Company name" and related assets, approved by the vendor's management? Does it include some of the following: • Request, review and approval of proposed changes • Review for potential security impact • Security approval • Review for potential operational impact • Approval from "Company name" (when applicable) • Documentation of changes • Pre-implementation testing • Post-implementation testing • Rollback procedures		
81	Operation Management	Does the vendor have a documented process for handling emergency changes in the "Company name" operation to ensure if such emergency changes are carried out in controlled & timely manner? Mention the details of the sample evidence.		
82	Operation Management	Does the Vendor have a mechanism to collect, analyse and store the logs of system such as F/w, Application Servers, Web Servers, End Point systems, Databases etc.? If yes, Mention the details of the mechanism.		
83	Operation Management	Do systems and network devices utilize a common time synchronization service?		
84	Operation Management	Are the system audit trail files protected from the unauthorized modifications or access ?		
85	Operation Management	Is there a process for taking secure back up of audit trail files to a centralized log server or media to prevent unauthorized access or alteration ? Are the backup for the audit trail files maintained.		
86	Operation Management	Are the "Company name" operations security logs reviewed?(Only applicable for Very critical process)		
87	Operation Management	Are the logs of Database activities and commands performed by the DBA team collected and analysed in the log management system?		
88	Operation Management	Does the vendor follow a maker-checker process for changes made to 1. Systems/Servers (Database, application server, web server, etc.) 2. Data (Business/functional)		
89	Operation Management	Does the vendor follow a maker-checker procedure for all the critical activities pertaining to "Company name"?		
90	Operation Management	Are capacity requirements monitored and regularly reviewed and systems and networks scaled accordingly?		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
91	Operation Management	Are backup media stored offsite?		
92	Operation Management	Is there a secure process for onsite & offsite backup media protection during storage pertaining to "Company name" operations? How is integrity assured for offsite backups?		
93	Operation Management	Does vendor have media labeling procedure in place, with sufficient information?		
94	Operation Management	Does the organization reuse, test & restore backups on regular basis?		
95	Operation Management	Is the data downloaded from uniken/seclore/sftp is stored securely after being downloaded and decrypted?(for both automated spool input files and the manual excel input files)		
96	Operation Management	Does the vendor have a secure mechanism for destruction & disposal of media / hardware used for "Company name" operations? Mention the details of the sample evidence.		
97	Personnel Security	Do you perform background verification for employees and contractors/temporary staff related to "Company name" scope of work? - Academic & professional Qualification - Police Verification - Reference check - Identification Check		
98	Personnel Security	The employment contract signed with the employees working on "Company name" scope of work should contain -Non-Disclosure Agreement; -Information Security responsibilities		
99	Personnel Security	Is the code of conduct performed by the vendor for their employees & is it in line with The Bank's code of conduct.		
100	Personnel Security	a. Does the vendor organization conduct pre-joining & periodic information security trainings & awareness programs to convey criticality of "Company name" data? b. Mention if there is a structured mechanism for disciplinary action against non-performers in trainings and otherwise.		
101	Physical & Environmental Security	Is there a structured process with defined responsibilities for removal of access rights & revoking of assets when person leaves "Company name" scope of work?		
102	Physical & Environmental Security	Are the critical servers related to "Company name" scope of work placed in secure area?		
103	Physical & Environmental Security	Is there appropriate segregation between "Company name" work area & other facility ?		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
104	Physical & Environmental Security	Is the physical entry / exit from the premises to "Company name" data processing facility & critical site monitored? If yes, specify the mechanism.		
105	Physical & Environmental Security	What type of Access control Mechanism is implemented for controlling access to "Company name" data processing facility ? (e.g.. Biometric / Access cards / Manual Registers)		
106	Physical & Environmental Security	a. In case of manual registers, is a log maintained to track / monitor the visit of other personnel in "Company name" data processing facility ? B. Are visitors accompanied by responsible escort personnel?		
107	Physical & Environmental Security	Are there procedures developed to easily distinguish between onsite personnel and visitors, especially in areas where "Company name" data is accessible.		
108	Physical & Environmental Security	Are Visitors asked to surrender the physical token before leaving the facility or at the date of expiration ?		
109	Physical & Environmental Security	Is there a defined policy or process to restrict the usage of personal storage device? If yes, mention the process to check for personal storage devices		
110	Physical & Environmental Security	Is there a process to restrict the usage of digital devices(mobile phone/tablets) or non digital materials (like paper, pen etc.) in Data Entry Area and other critical areas? (Critical for Call center setup, Card Processing but not limited to specified activities)		
111	Physical & Environmental Security	Are CCTV footages recorded and stored? What is the retention period defined for storing Access\CCTV logs?		
112	Physical & Environmental Security	Is there a role based access control for accessing critical facilities used for "Company name" operations?		
113	Physical & Environmental Security	What are the fire protection & detection mechanisms placed in critical IT locations including Data Center/ Server Room pertaining to "Company name" operations? Are environmental protection equipment's (heat detection, smoke detection, fire suppression, fireproofing, water flooding, heat, humidity, air conditioning, power supply) installed, tested, and monitored?		
114	Physical & Environmental Security	Is there an UPS mechanism / Power Generator in place at the Vendor site?		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
115	Physical & Environmental Security	Are the network and the power cable lines segregated physically?		
116	Service Delivery	Is vendor sub-contracting part of its services provided to "Company name"? Are contracts, Confidentiality Clause & SLA defined for the same? Does the contract refers to information security requirements for "Company name" data? Has the vendor obtained approval from bank for sub contracting?		
117	Service Delivery	How does vendor monitor the sub-contracting operations for "Company name" scope of work? -Onsite reviews		
118	Service Delivery	Does the contractual document with "Company name" include following at the minimum- -Scope -Performance standards -Access to books, records -Right to inspect & audit -Confidentiality & Security -Termination clause - Business Continuity -Dispute resolution -Applicable laws & regulatory guidelines -Subcontracting? -Information security clauses - Indemnity clause - obligation of the service provider - Publicity & proprietary rights - Insurance		
119	Service Delivery	Are you compliant with the Labour Law?		
120	Service Delivery	Are the confidentiality and non-disclosure agreements reflecting the organization's needs for the protection of information / data identified and reviewed?		
121	Service Delivery	Does the vendor have defined escalation mechanism for service outages & other issues?		
122	Service Delivery	How frequently is the review of compliance with SLA done for "Company name" operations?		
123	System Security	SCD: Are Security configuration standards for networks, operating systems, databases, applications and desktops defined?		
124	System Security	Are the systems used for "Company name" operations hardened according to hardening document/ technical specification document?		

Sr. no.	Control Area	Control Activity	Auditor's Remark	Auditee's Remark
125	System Security	Are the vendor-supplied default passwords changed before installing a system on the network? Are unnecessary accounts deleted on the network devices, servers and database etc. ? Mention the details of the sample evidence.		
126	System Security	Is there only one primary function per server implemented to prevent functions that require different security levels from co-existing on the same server? (For example, web servers, database servers, and DNS should be implemented on separate servers) for critical process/activities		

If you find it useful, Do follow

in/sachin-hissaria

@sachinhissaria6512

Thank you 🙏