

IT AUDIT PROJECT

“To create a checklist for all ITGCs along with the list of evidence required to test the controls.”

SUBMITTED BY

|  |  |
| --- | --- |
| **NAME** | **PRN** |
| ANKITA | 24030241161 |
| AKSHAT SINGHAI | 24030241158 |
| HARSH VARDHAN BAJAJ | 24030241173 |
| RASHMI KOUJALGI | 24030241192 |
| SAGAR SHARMA | 24030241195 |
| SUDARSHAN KHANDELWAL | 24030241202 |
| GRISHMA ARYA | 24030241172 |

SUBMITTED TO

**DR. VIDYAVATI RAMTEKE**

|  |  |
| --- | --- |
| **AUDIT DETAILS** | |
| AUDITING TEAM: | 1. ANKITA |
| 2. AKSHAT SINGHAI |
| 3. HARSH VARDHAN BAJAJ |
| 4. RASHMI KOUJALGI |
| 5. SAGAR SHARMA |
| 6. SUDARSHAN KHANDELWAL |
| 7. GRISHMA ARYA |
| NUMBER OF MEMBERS: | 07 |
| AUDIT OBJECTIVE: | To create a checklist for all the ITGCs and the list of evidence required to test the controls. |
| START DATE: | 15TH JANUARY 2025 |
| END DATE: | 19TH JANUARY 2025 |

**ITGC CHECKLIST**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **1.1** | Physical security should be ensured at all points in time to prevent attacks and external sources from coming and stealing data or harming the organization's assets. | **Physical Security Control (PSC)** | **PS-01** | Are server rooms secured with access control mechanisms? | **Preventive** | **Facilities Team** | **Examine:** Review access logs and badge records for anomalies, unauthorized entries, and compliance with access control policies.  **Interview:** Discuss with the access control team how logs are monitored and escalations are handled.  **Test:** Simulate unauthorized access and check if it is logged and flagged appropriately. |
| **1.2** | **PS-02** | Are CCTV cameras installed and operational in sensitive areas? | **Detective, Protective** | **Facilities Team** | **Examine:** Verify the availability and retention of CCTV logs, ensuring alignment with security policies.  **Interview:** Consult with the security team about the frequency and process of reviewing CCTV footage.  **Test:** Request specific footage to confirm accessibility and verify retention periods. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **1.3** |  |  | **PS-03** | Are fire suppression systems installed in data centers? | **Preventive** | **Facilities Team** | **Examine:** Check maintenance logs for completeness, frequency, and adherence to scheduled maintenance plans.  **Interview:** Talk to the maintenance personnel about procedures for maintaining IT systems and facilities.  **Test:** Inspect a recently maintained system or equipment to verify the accuracy of records. |
| **1.4** |  |  | **PS-04** | Are physical access rights reviewed periodically? | **Detective** | **Security officer IT security team** | **Examine:** Review logs to confirm regular access reviews and identify if inappropriate access was removed.  **Interview:** Engage with the access management team to understand the process and frequency of reviews.  **Test:** Perform a sample review of active user accounts to identify any access inconsistencies. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **1.5** |  |  | **PS-05** | Are visitor logs maintained for all restricted areas? | **Detective, Administrative** | **Facility management**  **Security officer** | **Examine:** Analyze visitor logs for completeness, timeliness, and adherence to visitor management policies.  **Interview:** Speak to reception or security personnel about the visitor check-in and verification process.  **Test:** Conduct a mock visitor entry to validate the logging and verification procedures. |
| **1.6** |  |  | **PS-06** | Are physical security breaches reported and investigated? | **Detective** | **Facilities Team** | **Examine:** Evaluate incident reports for proper documentation, timely resolution, and trend analysis.  **Interview:** Discuss with the incident response team the process for logging and addressing incidents.  **Test:** Simulate a minor incident to assess how it is reported and managed. |
| **1.7** |  |  | **PS-07** | Are backup power systems in place for critical facilities? | **Preventive, Compensative** | **Facility management**  **Security officer** | **Examine:** Check records of power system inspections and maintenance to confirm adherence to schedules.  **Interview:** Consult with the facilities team about power backup and maintenance protocols.  **Test:** Trigger a simulated power failure to ensure the system operates as documented. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **1.8** |  |  | **PS-08** | Is there a policy for handling lost or stolen access cards? | **Preventive, Administrative** | **Visitor Management officer**  **Security officer** | **Examine:** Review policy documents for relevance, version control, and alignment with organizational standards.  **Interview:** Discuss with management or the policy owner the process for creating and updating policies.  **Test:** Check compliance by comparing practices with the documented policies. |
| **1.9** |  |  | **PS-09** | Are physical security controls tested periodically? | **Detective** | **Facilities Team** | **Examine:** Assess test results and reports for accuracy, scope, and documentation of outcomes.  **Interview:** Speak to the testing team about methodologies and validation processes.  **Test:** Reperform a sample test to verify results and methodologies. |
| **1.10** |  |  | **PS-10** | Are restricted areas clearly marked and monitored? | **Preventive, Administrative** | **Facilities Team** | **Examine:** Analyze inspection reports for thoroughness, findings, and corrective actions.  **Interview:** Discuss with inspectors the areas of focus during their inspections.  **Test:** Verify inspection outcomes by cross-checking a sample area or equipment. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **1.11** |  |  | **PS-11** | Are there security guards stationed at critical locations? | **Preventive, Protective** | **Facilities Team** | **Examine: Review guard logs for shifts, incidents, and adherence to security protocols.**  **Interview: Engage with the security team to understand the logging process and escalation methods.**  **Test: Conduct an unannounced inspection to observe guard performance and logging accuracy.** |
| **1.12** |  |  | **PS-12** | Are environmental controls like HVAC monitored in data centers? | **Preventive, Protective** | **Security officer**  **Access control administrator** | **Examine: Evaluate logs from monitoring systems for completeness, frequency, and alerting mechanisms.**  **Interview: Speak to IT operations about how monitoring systems are configured and monitored.**  **Test: Generate a system anomaly to check if the monitoring system logs and alerts accurately.** |
| **1.13** |  |  | **PS-13** | Are all entry points equipped with alarm systems? | **Preventive** | **Security officer** | **Examine: Review test reports for alarms to confirm regular testing and proper functioning.**  **Interview: Discuss with the alarm management team the schedule and procedure for testing.**  **Test: Trigger an alarm as part of a drill to validate its functionality and response time.** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **1.14** |  |  | **PS-14** | Is there a process for deactivating access for terminated employees? | **Detective, Administrative** | **Security officer**  **Access control administrator** | **Examine:** Check records for timely removal of access rights for terminated employees or contractors.  **Interview:** Engage with the HR and IT teams to understand the access termination process.  **Test:** Review a sample of recent terminations to verify that access was revoked promptly. |
| **1.15** |  |  | **PS-15** | Are physical security policies reviewed annually? | **Detective, Administrative** | **Security officer** | **Examine:** Review minutes of policy review meetings for evidence of discussions and decisions.  **Interview:** Speak to participants about key issues addressed during policy reviews.  **Test:** Verify the implementation of changes decided upon during the review meetings. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **2.1** | **To ensure incidents are effectively logged, prioritized, escalated, resolved, and reported in accordance with defined policies and procedures.** | **Incident Management (IM)** | **IM-01** | Are all incidents logged in the system? | **Detective** | **IT Helpdesk Team** | **Examine:** Incident log reports for completeness and accuracy.  **Interview:** IT Helpdesk personnel to confirm logging practices**.**  **Test:** Attempt to log a test incident and verify its appearance in the system. |
| **2.2** | **IM-02** | Are incidents categorized based on severity? | **Preventive** | **IT Operations Team** | **Examine:** Incident categorization policy and guidelines.  **Interview:** IT Operations staff on severity classification process.  **Test:** Review sample incidents to verify proper categorization. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **2.3** |  |  | **IM-03** | Are escalation procedures documented? | **Preventive** | **IT Security Manager** | **Examine:** Escalation procedure document.  **Interview:** IT Security Manager on escalation practices.  **Test:** Simulate an incident to evaluate escalation effectiveness. |
| **2.4** | **IM-04** | Are incidents resolved within SLA timelines? | **Detective** | **IT Support Team** | **Examine:** SLA reports and resolution metrics.  **Interview:** IT Support Team about SLA adherence.  **Test:** Cross-check resolution times for sampled incidents against SLA targets. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **2.5** |  |  | **IM-05** | Is root cause analysis conducted for P1 issues? | **Corrective** | **Problem Management Team** | **Examine:** Root cause analysis reports for major incidents.  **Interview:** Problem Management Team on analysis methodology.  **Test:** Review a recent P1 incident and validate the root cause analysis process. |
| **2.6** | **IM-06** | Are incident reports shared with stakeholders? | **Preventive** | **IT Governance Team** | **Examine:** Incident summary reports shared with stakeholders.  **Interview:** IT Governance Team about reporting frequency.  **Test:** Verify distribution of incident reports for the last quarter. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **3.1** | **Verify the effectiveness of third-party risk management processes, including vendor assessment, compliance, contract management, monitoring, and data security.** | **TPRM** | **TPRM-01** | Is a formal risk assessment conducted for each vendor before onboarding? | **Preventive** | **Risk Management Team** | **Examine:** Collect vendor risk assessment reports, risk scoring documentation, and relevant policies. Validate whether the reports follow predefined organizational standards. **Interview:** Discuss with risk management personnel about the criteria and methodology used in assessing vendor risks. Identify decision points for vendor approval or rejection.  **Test:** Review recent risk assessment cases and cross-check if appropriate approvals were obtained. |
| **3.2** |  |  | **TPRM-02** | Are third parties assessed for compliance with applicable regulations (e.g., GDPR, ISO 27001)? | **Detective** | **Compliance Team** | **Examine:** Review compliance certificates (e.g., ISO 27001, GDPR) and recent regulatory audit reports from third parties. Verify the currency and validity of certifications.  **Interview:** Question compliance team members about processes for evaluating vendor adherence to regulations and standards. Understand how exceptions are managed. **Test:** Analyze audit trails and perform sampling to confirm compliance evidence is collected consistently. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **3.3** |  |  | **TPRM-03** | Are contracts with third parties reviewed to include confidentiality and security clauses? | **Preventive** | **Legal/Procurement Team** | **Examine:** Review executed contracts to confirm the inclusion of confidentiality and data protection clauses. Check for approval sign-offs on contract documents. **Interview:** Discuss with the legal and procurement teams how contracts are reviewed and monitored for security clauses. Identify any gaps in standard contract templates. **Test:** Select a random sample of vendor contracts and evaluate if all essential clauses are present and adhered to. |
| **3.4** |  |  | **TPRM-04** | Are vendors periodically monitored for performance and ongoing risk exposure? | **Detective** | **Vendor Management Team** | **Examine:** Evaluate vendor monitoring reports, including periodic SLA compliance documentation and performance summaries. Confirm adherence to monitoring schedules. **Interview:** Interact with vendor management teams to understand monitoring frequency, escalation procedures for SLA breaches, and handling of underperformance. **Test:** Trace SLA violations for select vendors and verify if corrective actions were executed within required timeline. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **3.5** |  |  | **TPRM-05** | Are data-sharing agreements in place, and do they meet organizational security standards? | **Preventive** | **IT Security Team** | **Examine:** Collect and validate data-sharing agreements to confirm alignment with organizational security standards. Review encryption requirements and compliance to data protection laws. **Interview:** Consult the IT security team on encryption methods, data-sharing approval processes, and periodic reviews. Identify vulnerabilities in the approval chain. **Test:** Simulate secure data exchange with a vendor to validate encryption protocols and agreement compliance. |
| **3.6** |  |  | **TPRM-06** | Do vendors have an incident response plan in case of a data breach or service disruption? | **Detective** | **IT Security Team** | **Examine:** Review documented incident response plans, breach reports, and response timelines provided by vendors. Verify if plans include communication protocols and escalation matrices. **Interview:** Discuss incident management processes with vendors and IT security teams. Identify how breaches are logged, managed, and resolved. **Test:** Request vendors to provide evidence of past incidents handled and validate their adherence to response protocols. |
| **3.7** |  |  | **TPRM-07** | Are vendors meeting agreed-upon service levels as defined in the SLA? | **Detective** | **Vendor Management Team** | **Examine:** Review SLA documentation and performance dashboards to verify vendor compliance with contractual obligations. Evaluate periodic reports for accuracy and completeness. **Interview:** Engage with vendor management to discuss escalation mechanisms for SLA violations and how penalties are enforced. **Test:** Reconcile SLA breach logs with action plans and validate corrective actions taken by the vendor. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **3.8** |  |  | **TPRM-08** | Are there procedures in place to ensure smooth termination of vendor relationships? | **Preventive** | **Risk Management Team** | **Examine:** Verify vendor termination documents, including data retrieval and offboarding checklists. Confirm presence of clauses for returning sensitive data. **Interview:** Speak with the risk team to understand the procedures for offboarding vendors, ensuring continuity, and addressing data disposal. **Test:** Simulate a vendor offboarding scenario and confirm adherence to termination protocols. |
| **3.9** |  |  | **TPRM-09** | Are vendors required to assess and monitor their subcontractors for risks? | **Preventive** | **Vendor Management Team** | **Examine:** Review subcontractor risk assessments, vendor attestations, and contractual provisions governing subcontractor activities. **Interview:** Interact with vendor managers to discuss how subcontractors are assessed and managed. Identify reporting mechanisms. **Test:** Request subcontractor compliance reports and verify alignment with main vendor agreements. |
| **3.10** |  |  | **TPRM-10** | Do vendors have business continuity plans to ensure uninterrupted services? | **Detective** | **Business Continuity Team** | **Examine:** Review vendor business continuity plans (BCPs) and test results. Verify inclusion of risk mitigation strategies for service disruptions. **Interview:** Speak with continuity planners to assess preparedness for high-risk scenarios. Discuss frequency and scope of testing. **Test:** Conduct tabletop exercises or request recent test results from the vendor to validate BCP effectiveness |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **4.1** | **The primary goal of**  **logical access controls**  **is to restrict access to**  **information assets,**  **thereby protecting**  **computer systems,**  **data, applications, and services from unauthorized access.** | **Logical Access Control (LAC)** | **LAC-01** | Is there any well-defined clause for access control in cyber security policy? | **Deterrent** | **IT Security team** | **Examine:** Review the organization's cyber security policy document to identify and extract any explicitly defined clauses related to access control.  **Interview:** Speak with the Information Security Officer or the person responsible for policy development to understand the intent and details of the access control clauses within the cyber security policy.  **Test:** Assess the implementation of access control measures by validating that they align with the specifications outlined in the cyber security policy through technical evaluations and system audits. |
| **4.2** |  |  | **LAC-02** | Are the user privileges altered as per their roles/ positions? | **Preventive** | **Security Administrator** | **Examine:** Review access control policies and documentation to verify alignment with defined user roles and positions.  **Interview:** Conduct discussions with system administrators and security personnel to gather insights on the process of assigning user privileges based on roles and positions.  **Test:** Perform access control tests by simulating changes in user roles and positions to ensure that corresponding privilege alterations are accurately implemented in the system |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **4.3** |  |  | **LAC-03** | Does the security policy get updated as the company works on different projects from different | **Detective** | **Chief Information Security Officer (CISO)** | **Examine:** Review the version history or change log of the security policy documentation to identify and verify updates or revisions made during and after the completion of projects from different domains.  **Interview:** Interview key stakeholders involved in project management, security, and policy enforcement to understand the process of updating the security policy and whether it is aligned with the initiation and completion of projects across various domains. **Test:** Conduct a comparison between the security policy versions before and after the completion of projects, ensuring that updates are evident and address specific security considerations related to the diverse domains in which the company operates. |
| **4.4** |  |  | **LAC-04** | Is the company following ISO27002:2013 or equivalent standards for good practice? (e.g., Check for password related standards) | **Preventive** | **Chief Information Security Officer (CISO)** | **Examine:** Review documented policies and procedures related to information security to verify alignment with ISO 27002:2013 or equivalent standards.  **Interview:** Interview key personnel responsible for information security, such as the Information Security Officer, to inquire about the organization's adherence to ISO 27002:2013 and specifically its password-related standards.  **Test:** Conduct a technical assessment by examining the implemented access control and password management systems to ensure they align with the requirements specified in ISO 27002:2013 or equivalent standards. |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **4.5** |  |  | **LAC-05** | Is it true that invalid login attempts are tracked and user-ids are suspended based on the kind of attempt? | **Detective** | **Chief Information Security Officer (CISO)** | **Examine:** Review the access control system logs and reports to identify records of invalid login attempts, focusing on timestamps, user IDs, and the type of attempts (e.g., incorrect passwords, brute force attacks).  **Interview:** Conduct interviews with system administrators or security personnel to inquire about the organization's policies and procedures regarding the tracking of invalid login attempts and the suspension of user IDs based on the nature of the attempt.  **Test:** Simulate various invalid login scenarios, including incorrect passwords and potential brute force attacks, and observe the system's response to validate that it tracks such attempts and appropriately suspends user IDs in accordance with the security policies |
| **4.6** |  |  | **LAC-06** | Is there multifactor authentication for different administrative accounts? | **Preventive** | **Chief Information Security Officer (CISO)** | **Examine:** Review system configuration settings and documentation to identify if multi-factor authentication (MFA) is enabled for administrative accounts.  **Interview:** Speak with system administrators and IT personnel to confirm the use of multi-factor authentication and inquire about the methods in place for different administrative accounts.  **Test:** Conduct simulated login attempts on administrative accounts and verify if multifactor authentication prompts are triggered as expected. |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **4.7** |  |  | **LAC-07** | Whether the organization has restricted concurrent logon from different devices/  locations? | **Deterrent** |  | **Examine:** Review the organization's access control policy or configuration settings to identify any documented restrictions on concurrent logon from different devices or locations.  **Interview:** Engage with the IT security team or relevant personnel to inquire about the specific measures in place to restrict concurrent logon from different devices or locations, and confirm the information gathered through policy review.  **Test:** Conduct a technical assessment by attempting concurrent logons from different devices or locations to verify if the access control system effectively enforces restrictions as stated in the organization's policies and configurations. |
| **4.8** |  |  | **LAC-08** | Are there restrictions to downloading/  installing any unauthorized software? | **Deterrent** | **IT Security team** | **Examine:** Review the organization's IT policies and documentation to identify explicit restrictions on downloading or installing unauthorized software.  **Interview:** Speak with IT administrators or relevant personnel to inquire about any formal procedures or controls in place to prevent the download and installation of unauthorized software.  **Test:** Conduct a controlled test by attempting to download and install software that is not on the approved list, and observing the system's response and any implemented restrictions. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **5.1** | **Ensure critical system operations are monitored, maintained, secured, and documented with robust processes for performance tracking, disaster recovery, backup testing, patch management, log archiving, incident escalation, and audit trails to guarantee availability, reliability, and traceability.** | **System Operations (SOC)** | **SOC-01** | Are critical systems monitored 24/7? | **Detective** | **IT Operations** | **Examine:** Monitoring logs and alerts. **Interview:** Discuss monitoring procedures with the IT team. **Test:** Simulate an issue and check if alerts are generated and escalated. |
| **5.2** |  |  | **SOC-02** | Are scheduled maintenance activities documented? | **Preventive** | **IT Operations** | **Examine:** Maintenance schedules and reports.  **Interview:** Verify with maintenance staff about adherence to schedules. **Test:** Review completion of recent scheduled activities. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **5.3** |  |  | **SOC-03** | Are performance metrics for critical systems tracked? | **Detective** | **IT Operations** | **Examine:** Performance monitoring reports. **Interview:** Ask IT staff about metric thresholds and monitoring tools.  **Test:** Verify consistency in reported metrics against logs. |
| **5.4** |  |  | **SOC-04** | Are system configurations documented and reviewed? | **Preventive** | **IT Operations** | **Examine:** Configuration documentation and review logs. **Interview:** Confirm with the configuration team about review processes. **Test:** Check for discrepancies in configurations. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **5.5** |  |  | **SOC-05** | Is there a disaster recovery plan (DRP) in place? | **Preventive** | **IT Operations** | **Examine:** DRP documentation and test results. **Interview:** Discuss the DRP with the team.  **Test:** Conduct a simulated DRP scenario and validate recovery time objectives (RTOs). |
| **5.6** |  |  | **SOC-06** | Are backups tested periodically for recoverability? | **Detective** | **IT Operations** | **Examine:** Backup logs and test results**. Interview:** Verify backup policies with administrators. **Test:** Restore a backup and ensure data integrity. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **5.7** |  |  | **SOC-07** | Are critical patches applied in a timely manner? | **Preventive** | **IT Operations** | **Examine:** Patch management records. **Interview:** Confirm patch schedules and criticality assessment processes.  **Test:** Review timelines for applying recent critical patches. |
| **5.8** |  |  | **SOC-08** | Are system logs archived securely? | **Preventive** | **IT Operations** | **Examine:** Log archival policies and retention schedules. **Interview:** Ask IT team about access controls for archived logs. **Test:** Retrieve an archived log and validate security. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **5.9** |  |  | **SOC-09** | Is there a process for incident escalation and resolution? | **Corrective** | **IT Operations** | **Examine:** Incident records and escalation workflows. **Interview:** Verify procedures with the incident response team. **Test:** Simulate an incident and validate escalation steps. |
| **5.10** |  |  | **SOC-10** | Are audit trails enabled for critical systems? | **Detective** | **IT Operations** | **Examine:** Audit trail logs and monitoring tools. **Interview:** Discuss audit trail review processes with the team. **Test:** Trigger an event and verify if it is recorded in the audit log. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **6.1** | **Ensure the effectiveness and security of backup management processes by validating adherence to backup policies, continuous monitoring, segregation of environments, data integrity, disaster recovery preparedness, access controls, encryption mechanisms, storage utilization trends, incident response for backup failures, and schedule efficiency.** | **Data Backup and Recovery** | **DB-01** | Is the backup policy reviewed and updated regularly to address emerging risks? | **Preventive** | **IT Operations** | **Examine:** Review backup policy documents and revision history.  **Interview:** Discuss with policy owners on update frequency.  **Test:** Verify if the updated policy addresses new risks or requirements. |
| **6.2** |  |  | **DB-02** | Are real-time monitoring systems implemented to detect backup system failures? | **Detective** | **IT Team** | **Examine:** Inspect monitoring tool configurations and logs.  **Interview:** Confirm monitoring practices with system administrators.  **Test:** Simulate a failure and check if alerts are generated. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **6.3** |  |  | **DB-03** | Are production, staging, and development backup environments logically segregated? | **Preventive** | **Data Protection Manager** | **Examine:** Review environment configuration settings and diagrams.  **Interview:** Speak with administrators about environment access controls.  **Test:** Attempt cross-environment access to validate segregation. |
| **6.4** |  |  | **DB-04** | Are data integrity checks performed on backup files after every backup operation? | **Detective** | **Quality Assurance Team** | **Examine:** Check integrity check reports and error logs.  **Interview:** Ask QA team about integrity validation procedures.  **Test:** Perform an integrity check on a sample backup file. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **6.5** |  |  | **DB-05** | Are backup copies tested as part of the disaster recovery drills? | **Preventive** | **Business Continuity Manager** | **Examine:** Review disaster recovery drill documentation and results.  **Interview:** Discuss drill execution with relevant teams.  **Test:** Participate in or observe a scheduled drill. |
| **6.6** |  |  | **DB-06** | Are role-based access controls enforced for accessing backup systems? | **Preventive** | **IT Team** | **Examine:** Audit access control logs and system roles. **Interview:** Confirm with IT administrators about access management processes.  **Test:** Attempt unauthorized access to verify restrictions. |
| **6.7** |  |  | **DB-07** | Are encryption keys used for backups rotated periodically and securely stored? | **Preventive** | **IT Operations** | **Examine:** Review encryption key rotation logs and storage procedures.  **Interview:** Confirm with the encryption team about key management practices.  **Test:** Validate the encryption key rotation process by inspecting a recent key change. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **6.8** |  |  | **DB-08** | Are storage usage trends analyzed to ensure sufficient capacity for future backups? | **Detective** | **Network Manager** | **Examine:** Review storage utilization reports and capacity plans. **Interview:** Speak with the network team about monitoring practices. **Test:** Verify available capacity and simulate a high-usage scenario. |
| **6.9** |  |  | **DB-09** | Are documented incident response procedures followed in the event of a backup failure? | **Detective** | **Data Protection Manager** | **Examine:** Inspect incident logs and response documentation. **Interview:** Confirm with the response team about standard procedures followed. **Test:** Analyze a recent incident to confirm compliance with the procedure. |
| **6.10** | |  | | --- | |  | |  | **DB-10** | Are backup schedules optimized to minimize impact on system performance during critical hours? | **Preventive** | **IT Operations** | **Examine:** Review backup schedules and system performance reports. **Interview:** Discuss optimization strategies with IT Operations. **Test:** Monitor system performance during a scheduled backup. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **7.1** | **Change Management Control is responsible for ensuring that any existing and planned change to the IT system assets, applications, and even infrastructure is properly approved, tested and documented.** | **Change Management (CM)** | **CM-01** | Are all changes logged through a formal request process? | **Preventive** | **Change Management Team** | **Examine**: Change request logs for completeness, unique IDs, and business justification.  **Interview**: Change management team on logging practices.  **Test**: Submit a sample change request and verify its logging. |
| **7.2** |  |  | **CM-02** | Are changes approved by authorized personnel? | **Preventive** | **Change Manager** | **Examine:** Approval workflows and records in the change management system. **Interview:** Approvers about their reviewprocess**. Test:** Review some sample change requests to ensure that approvals are in place. |
| **7.3** | |  | | --- | |  | |  | **CM-03** | Are changes tested in a non-production environment? | **Preventive** | **QA/Testing Team** | **Examine:** Test plan, results and coverage documentation**.**  **Interview:**QA team on environment segregation and testing protocols.  **Test:** Simulate a change and analyze test results in the non-production environment. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **7.4** |  |  | **CM-04** | Are rollback plans documented for all changes? | **Preventive** | **Change Owner** | **Examine:** Rollback procedures in the changetickets**. Interview:** Change owner on rollback readiness. **Test:** Request a rollback simulation for a selected change. |
| **7.5** |  |  | **CM-05** | What is the process for reviewing and approving changes? | **Preventive** | **Change Management Officer** | **Examine:** Approvals in the change management system Record of change requests with proper approvals, either in signed paper formats or electronic form Audit trail detailing the sequence of reviews and approvals  **Interview:** Change Management officer and team who reviewed and approved the changes Ask them about the criteria used in approving or rejecting a particular change  **Test:** Choose a sample of recent change requests and confirm that appropriate review and approval steps were taken. Simulate a change request and see whether it follows the defined approval workflow. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SR. NO** | **AUDIT REQUIREMENTS** | **CONTROL CATEGORY** | **CONTROL**  **IDs** | **QUESTIONS** | **CONTROL TYPE** | **CONTROL OWNER** | **EVIDENCE REQUIRED** |
| **7.6** |  |  | **CM-06** | Are changes reviewed post-implementation? | **Detective** | **Change Management Officer** | **Examine:**post-implementation review reports and identified issue logs.  **Interview:** Stakeholders on the review process.  **Test:** Verify a recent change review to ensure issues were resolved effectively. |
| **7.7** |  |  | **CM-07** | Is there a formal change management policy in place? | **Preventive** | **Change Management Officer** | **Examine:** Change management policy document and version control logs. **Interview:** Governance Team, Policy Changes. **Test:**Check whether the practice follows the policy documented. |
| **7.8** |  |  | **CM-08** | Are emergency changes documented and retroactively approved? | **Detective** | **IT Operations Manager** | **Examine:** Logs of emergency changes and retroactive approvals.  **Interview:** IT operations team on emergency change handling.  **Test:** Review a recent emergency change for documentation and post-implementation approval. |