IT AUDIT CHECKLIST

Domain
Security Policy
Organizational Security
Asset Management
Human Resource Security
Physical and Environmental Security
Communications and Operations Management
Access Control
Information Systems Acquisition, Development, and Maintenance
Information Security Incident Management
Business Continuity Management
Compliance

SACHIN HISSARIA
CA | CISA | DISA | CEH | COBIT-19 | ISO27001:2022 | RPA

Assessment Category	Assessment Sub-Category	Assessment Items	Status	Findings
Security Policy	Security Policy Documentation	Is there a documented information security policy in place?		
		Is the policy approved by management?		
		Is the policy communicated to all employees and relevant external parties?		
		Does the policy include definitions of information security responsibilities?		
		Is there a regular review and update process for the security policy?		
		Is there a defined consequence for non-compliance with the policy?		
		Are policies in line with business needs, relevant laws, and regulations?		
		Does the policy cover all necessary aspects of information security?		
	Security Policy Review	Is the policy reviewed at planned intervals?		
		Is the policy updated based on the results of audits, changes in business requirements, or changes in legal regulations?		
		Are revisions to the policy documented?		
		Are changes to the policy communicated in a timely manner to all relevant parties?		
		Is there a formal process for individuals to suggest improvements to the policy?		
		Are there measures in place to ensure continued policy effectiveness?		
		Are changes in technology considered during policy reviews?		
		Is there an appropriate response to significant security incidents that might lead to a policy review?		
	Security Policy Implementation	Is the policy implemented throughout the organization?		
		Are employees trained on the details of the policy and their individual responsibilities?		
		Is policy compliance monitored and enforced?		
		Is there an ongoing awareness campaign to keep the policy top-of-mind for employees?		
		Are resources allocated to facilitate policy implementation?		
		Are controls and processes aligned with policy requirements?		
		Are exceptions to the policy managed and approved through a formal process?		
		Is there a measure of the effectiveness of the policy implementation?		
Organizational Security	Internal Roles and Responsibilities	Are the roles and responsibilities for information security defined within the organization?		
		Are these roles and responsibilities communicated to the relevant personnel?		
		Are they included in job descriptions or contracts?		
		Is there a designated person or group in charge of information security management?		
		Are there clear reporting lines for security incidents or concerns?		
		Are segregation of duties principles applied to reduce the risk of unauthorized activities?		
		Is there a process for reviewing and updating roles and responsibilities?		
		Is the effectiveness of the roles and responsibilities implementation assessed?		
	External Roles and Responsibilities	Are information security requirements defined and communicated to external parties such as suppliers and contractors?		
		Are these requirements reflected in contracts and agreements?		
		Is there a procedure for managing changes in relationships with external parties?		
		Are there mechanisms for monitoring external parties' compliance with security requirements?		
		Are the consequences of non-compliance stated in contracts?		
		Are there regular security audits or reviews for third-party vendors?		
		Is there a procedure for terminating access to information assets when an external relationship ends?		
		Are there measures in place to assess third-party risk?		
	Security Awareness and Training	Is there a security awareness program for all employees?		
		Is the program tailored to different roles within the organization?		
		Is there a process to evaluate the effectiveness of the program?		
		Are there regular updates or refresher courses available?		
		Are new employees given security awareness training as part of their onboarding process?		
		Are there clear instructions on what to do in the event of a security incident?		
		Is there an ongoing campaign to keep security in the minds of employees?		
		Are there mechanisms to ensure third-party vendors receive appropriate security training?		

Assessment Category	Assessment Sub-Category	Assessment Items	Status	Findings
Asset Management	Inventory of Assets	Is there an inventory of all information assets?		
		Does the inventory include details of asset owners, locations, and classifications?		
		Is the inventory regularly reviewed and updated?		
		Is there a process to add and remove assets from the inventory as they come into or leave the organization?		
		Are there procedures in place to handle sensitive information assets?		
		Are all assets, including those owned by third parties but used by the organization, included in the inventory?		
		Are there controls in place to prevent unauthorized access to the inventory?		
		Are there measures in place to ensure the accuracy and completeness of the inventory?		
	Ownership of Assets	Are all assets owned by a designated part of the organization or individual?		
		Are asset owners aware of their responsibilities?		
		Are there processes for transferring ownership when necessary?		
		Are asset owners responsible for implementing appropriate security controls?		
		Is the asset owner responsible for maintaining an accurate inventory of their assets?		
		Is asset ownership documented and updated regularly?		
		Are there measures to ensure that asset ownership responsibilities are fulfilled?		
		Do asset owners have the authority to manage risks associated with their assets?		
	Classification and Control	Is there a classification scheme for information assets?		
		Are the classifications based on the value, legal requirements, sensitivity, and criticality to the organization?		
		Are asset owners responsible for classifying their assets?		
		Are there controls in place to ensure that assets are appropriately labeled and handled according to their classification?		
		Is the classification scheme regularly reviewed and updated?		
		Are employees trained on the classification scheme and handling procedures?		
		Is the impact of the loss, disclosure, alteration, or unavailability of assets considered in the classification?		
		Are there procedures to declassify or dispose of information assets?		
Human Resource Security	Prior to Employment	Are the roles and responsibilities for information security included in job descriptions?		
		Are employment contracts/agreements including appropriate terms for information security?		
		Is background verification carried out as part of the recruitment process, based on the risk of the job role?		
		Are all employees given a copy of the information security policy and adequately briefed?		
		Are non-disclosure agreements used where appropriate?		
		Is there a defined process for granting and revoking access rights for new employees?		
		Are there controls in place to identify potential insider threats during the recruitment process?		
		Is there a process to periodically verify the information security awareness of new employees?		
	During Employment	Are there programs in place to raise and maintain employee awareness about information security?		
		Are there procedures to monitor and respond to breaches of information security by employees?		
		Are information security expectations included in performance reviews?		
		Is there a disciplinary process for violation of information security policies?		
		Are changes in a role or responsibility accompanied by a review and adjustment of access rights?		
		Are there refresher training courses to keep employees updated on the latest threats and security practices?		
		Is there a procedure for handling suspected or observed employee misconduct related to information security?		
		Are there regular audits of user activity, especially those with elevated access privileges?		

Assessment Category	Assessment Sub-Category	Assessment Items	Status	Findings
	Termination or Change of Employment	Are there procedures for revoking access rights when an employee leaves the organization or changes job roles?		
		Is there a formal process for the return of organizational assets upon termination of employment?		
		Is there a procedure to remove all user accounts and credentials associated with an ex-employee?		
		Are exit interviews conducted to remind leaving employees of their ongoing responsibilities for information security?		
		Are there procedures in place to secure proprietary information after employee departure?		
		Is there a process for updating tasks and responsibilities that were assigned to a terminated employee?		
		Is there a procedure to monitor for suspicious activities related to an employee's impending departure?		
		Are there measures in place to ensure the continuity of necessary operations after an employee's departure?		
Physical and Environmental Security	Secure Areas	Are there designated secure areas to protect critical or sensitive information assets?		
		Are there controls in place to prevent unauthorized access to secure areas?		
		Are access rights to secure areas regularly reviewed and updated?		
		Are there measures to protect secure areas from physical threats such as fire, flood, etc.?		
		Are there procedures in place for visitors, including sign-in, escorts, and badge requirements?		
		Is there CCTV or other surveillance equipment to monitor secure areas?		
		Are there measures in place to prevent eavesdropping or unauthorized information gathering in secure areas?		
		Is there a process to assess the physical security measures of third-party vendors with access to sensitive information?		
	Equipment Security	Are there policies in place for using and maintaining organizational equipment securely?		
		Are there procedures to prevent theft, damage, and unauthorized access to organizational equipment?		
		Are there rules in place for removing equipment from the organization's premises?		
		Are there controls to protect equipment and power cables from physical and environmental threats?		
		Is there a secure disposal or reuse process for equipment?		
		Is there a process for managing equipment maintained by third parties?		
		Is there a system in place to maintain up-to-date inventory of all equipment?		
		Are all types of equipment (e.g., IT equipment, security equipment, etc.) covered under the equipment security policy?		
	Operational Procedures	Are operational procedures documented, maintained, and available to all users who need them?		
		Are duties segregated to reduce the risk of negligent or deliberate system misuse?		
		Are there procedures in place to control the installation of software on operational systems?		
		Are changes to operational systems controlled and documented?		
		Are output data validated to ensure the process is not compromised?		
		Is there an incident response procedure in place?		
		Is there a regular review process for operational procedures?		
		Are there procedures to control the implementation of patches and updates?		
	Third-Party Service Delivery Management	Are there controls and procedures for identifying and managing risks associated with third-party services?		
		Are third-party services outlined and controlled in contracts or agreements?		
		Are there procedures for monitoring and reviewing third-party services?		
		Are third-party access rights regularly reviewed and updated?		
		Is there a process for handling breaches of contract by third-party service providers?		
		Are there defined and agreed upon service levels?		
		Is there a procedure to ensure the secure disposal or return of assets at the termination of a contract?		
		Are there contingency plans in case the third-party provider fails to deliver?		

Assessment Category	Assessment Sub-Category	Assessment Items	Status	Findings
Communications and Operations Management	System Planning and Acceptance	Are there performance criteria defined during the planning and acceptance process of new systems?		
		Are information security aspects considered during system planning?		
		Is there a capacity management process in place?		
		Is acceptance testing performed for new systems, upgrades, and new versions?		
		Are the results of acceptance testing documented and reviewed?		
		Are there procedures in place to ensure that each system is appropriately licensed?		
		Are there procedures to ensure systems compatibility?		
		Is there a process to evaluate the system's adherence to information security policies?		
	Protection from Malware	Is there a policy to protect the organization from malware threats?		
		Are anti-malware software and signatures regularly updated?		
		Are there procedures to respond to a detected malware infection?		
		Is awareness training provided to staff regarding the risks associated with malware?		
		Are there controls in place to prevent and detect malware on user devices, servers, and network devices?		
		Are there protections against zero-day threats?		
		Is there regular scanning and removal of malware from websites, mail servers, and other systems?		
		Are there measures in place to prevent malware spread in the internal network?		
	Backup	Is there a policy and procedure for conducting regular backups?		
		Are backups regularly tested to ensure they are functioning correctly?		
		Are backups stored offsite and/or in a secure remote location?		
		Are backups encrypted?		
		Are backup procedures aligned with the organization's business continuity plan?		
		Are backup schedules based on the value and changes to the information?		
		Are there backup strategies for critical information and systems?		
		Is there a procedure in place for secure disposal of backup media?		
	Network Security	Are there controls in place to protect information systems from network threats?		
		Are there firewall and gateway controls in place at each network boundary?		
		Are there intrusion detection and prevention measures?		
		Are security features, service levels, and management requirements of all network services identified and included in any network services agreements?		
		Are there measures to segregate groups of information services, users, and information systems on the network?		
		Are there policies on the use of network services?		
		Is there routine network monitoring and logging?		
		Are there regular vulnerability scans and penetration tests on the network infrastructure?		
	Media Handling	Are there procedures in place for the secure handling, storage, and disposal of media?		
		Are media containing sensitive information securely disposed of when no longer required?		
		Are there procedures to prevent unauthorized access, damage, and theft to information stored on media?		
		Are backups of important media regularly made and securely stored?		
		Is there a policy that prohibits the removal of media from the organization without authorization?		
		Is sensitive information erased from media prior to disposal or reuse?		
		Are there procedures for the secure transfer of media and information?		
		Is all media clearly marked to indicate any sensitivities and the need for special handling?		

Assessment Category	Assessment Sub-Category	Assessment Items	Status	Findings
Access Control	Exchange of Information	Are there formal exchange policies, procedures, and controls in place to protect the exchange of information through all types of communication?		
		Are there agreements with external parties regarding the secure exchange of information and media?		
		Are sensitive documents classified and protected in accordance with this classification?		
		Are there secure methods used for the exchange of information, such as encryption?		
		Are physical media sent by courier or post properly protected?		
		Are there procedures in place to verify the identity of the receiver before sending sensitive information?		
		Are there procedures for dealing with misrouted or misaddressed information?		
		Are there procedures in place for the secure disposal or reuse of equipment used for information transfer?		
	Electronic Commerce	Are there security controls in place to protect electronic commerce processes?		
		Are all relevant legal requirements in relation to electronic commerce met?		
		Are there controls in place to detect and prevent fraudulent activities?		
		Are electronic commerce services regularly reviewed for compliance with the organization's security policy and standards?		
		Is there secure storage and transmission of customer data during electronic commerce transactions?		
		Are the confidentiality and integrity of information maintained during transaction processing?		
		Are there controls to prevent the repudiation of an electronic commerce transaction?		
		Are electronic commerce services regularly tested for security vulnerabilities?		
	User Access Management	Is there a formal user registration and de-registration process in place for granting and revoking access to all systems and services?		
		Are there procedures to assign access rights to all users and service providers, based on a minimal privilege principle?		
		Is there a process for managing the allocation of secret authentication information?		
		Are there processes in place for the review and update of user access rights at regular intervals?		
		Are there processes for removing or disabling user access rights when a user leaves the organization or changes jobs?		
		Is there a policy in place for the use of system utilities that could potentially override system and application controls?		
		Are there controls in place to manage the use of privileged utility programs?		
		Are there controls in place to restrict and monitor the allocation and use of privileged access rights?		
	User Responsibilities	Are users aware of their responsibilities for maintaining effective access controls, such as password management?		
		Is there a policy defining secure log-on procedures?		
		Are users accountable for their actions on the system?		
		Are users aware of the information access level they have and the corresponding responsibilities?		
		Are there policies in place to prevent the unauthorized use of information processing facilities?		
		Are there procedures for reporting any suspected security weaknesses or incidents?		
		Is the use of utility programs that could potentially bypass system and application controls restricted and controlled?		
		Is there a policy against sharing user credentials?		
	Network Access Control	Are there policies and procedures for protecting information systems from unauthorized network access?		
		Is there a secure log-on process for networks and network services?		
		Are there controls to manage the connection of mobile devices to the network?		
		Is network access granted based on a least privilege principle?		
		Are there controls in place to prevent network traffic from systems that do not need to connect to the network?		
		Are the use of active network services (such as email, internet, databases) controlled and properly protected?		
		Are network segregation controls in place?		
		Are network users authenticated?		

Assessment Category	Assessment Sub-Category	Assessment Items	Status	Findings
Information Systems	Operating System Access Control	Are there procedures in place to prevent unauthorized access to operating systems?		
		Is there a secure log-on process in place for access to operating systems?		
		Are all operating system access rights reviewed and updated on a regular basis?		
		Is the use of system utilities controlled?		
		Are session time-out controls implemented?		
		Are there restrictions on the connection of mobile devices and external storage devices?		
		Are password management systems interactive and ensure quality passwords?		
		Are all activities performed by privileged roles logged and monitored?		
	Application Access Control	Are there procedures in place to prevent unauthorized access to applications?		
		Is there a secure log-on process in place for access to applications?		
		Are all application access rights reviewed and updated on a regular basis?		
		Are session time-out controls implemented for applications?		
		Is there a policy against the use of application system utilities that might be capable of overriding system and application controls?		
		Are restrictions in place on information input via applications?		
		Are all activities performed within applications by privileged roles logged and monitored?		
	Monitoring System Access and Use	Is there an established process for monitoring and logging system access and user activities?		
		Are all logged events reviewed regularly?		
		Are system logs protected against tampering and unauthorized access?		
		Are the clocks of all relevant information processing systems synchronized?		
		Are there measures to collect and store evidence to support event analysis and legal action?		
		Are event logging and the protection of log information minimally compliant with legal requirements?		
		Are procedures in place to link all access to systems and procedures with individual users?		
		Are procedures in place to respond rapidly to anomalies?		
	Security Requirements of Information Systems	Is there an information security requirements analysis and specification process in place for all systems?		
		Is there a process for ensuring that all information processing systems meet the organization's information security requirements?		
		Is there a process for defining and implementing controls to ensure the accuracy and completeness of information outputs?		
		Are there regular checks to verify whether the security requirements of installed systems are being met?		
		Is there a regular review of the organization's business processes, information flows, and systems?		
		Are there processes in place to identify and assess risks to systems?		
		Is there a process in place to ensure that changes in the business and external environment are reflected in the systems' security requirements?		
		Are there procedures in place for the secure development and testing of systems?		
	Correct Processing in Applications	Are there controls to ensure correct processing in applications?		
		Are there procedures in place for detecting and correcting errors in processing?		
		Are there procedures in place for ensuring data integrity during processing?		
		Are there controls in place to prevent or detect the unauthorized manipulation of software?		
		Is there a process for ensuring that transaction errors are detected and handled appropriately?		
		Are there checks in place to verify the completeness and accuracy of processing?		
		Are there controls in place to ensure the authenticity and integrity of inputs and outputs?		
		Is there a rollback procedure for handling processing errors?		
	Cryptographic Controls	Is there a policy on the use of cryptographic controls?		
		Are cryptographic keys securely managed?		
		Are cryptographic controls used in compliance with all relevant agreements, legislation, and regulations?		
		Are cryptographic controls regularly reviewed and updated?		
		Is encryption used for the transmission of sensitive data over public networks?		
		Are there procedures in place for the use of digital signatures?		

Assessment Category	Assessment Sub-Category	Assessment Items	Status	Findings
Acquisition, Development, and Maintenance		Is the integrity of sensitive or critical information ensured using cryptographic techniques?		
		Are there controls in place to protect sensitive data in storage using cryptographic techniques?		
	Security of System Files	Are there controls in place to secure system files?		
		Is there access control in place to protect system files?		
		Are there controls to ensure the integrity of system files?		
		Is there a process for the secure development and testing of system files?		
		Is there a process in place to restrict the installation of software on operational systems?		
		Are there controls in place to manage system changes and upgrades?		
		Are system files regularly checked for malware and unauthorized changes?		
		Are there procedures in place for the secure disposal or reuse of storage media?		
	Security in Development and Support Process	Are there secure development policies in place?		
		Is there a formal change control process?		
		Are there technical reviews of applications after operating system changes?		
		Are there restrictions on changes to software packages?		
		Are there controls on information leakage from system development environments to operational environments?		
		Are there controls to ensure the separation of duties between developers and operational staff?		
		Is there a secure system engineering methodology in place?		
		Is there a formal process in place for system acceptance?		
	Technical Vulnerability Management	Are there procedures for timely information collection about technical vulnerabilities?		
		Are the organization's exposure to such vulnerabilities evaluated?		
		Is there a process for timely remediation of the identified vulnerabilities?		
		Are there controls to restrict the exploitation of technical vulnerabilities?		
		Are vulnerabilities regularly checked through penetration testing or vulnerability assessments?		
		Are patches for vulnerabilities applied in a timely manner?		
		Is there an established process for verifying the security of outsourced development?		
		Are there measures to protect against malicious code and back doors in software?		
Information Security Incident Management	Reporting Information Security Incidents	Is there a formal event reporting and escalation process?		
		Are users and system managers aware of their responsibility for reporting information security incidents immediately?		
		Are there procedures for reporting software malfunctions?		
		Are there mechanisms for reporting security incidents to external organizations where relevant (e.g., cybercrime reporting)?		
		Are all employees trained to recognize and report incidents?		
		Is there a process for reporting the loss or compromise of information assets?		
		Are there measures in place to minimize damage from incidents and to restore systems to normal operation as quickly as possible?		
		Is there a feedback loop in place to learn from incidents and implement improvements?		
	Management of Information Security Incidents and Improvements	Is there a process for responding to and managing information security incidents?		
		Is there a process for implementing necessary improvements to organizational policies and procedures following an incident?		
		Is there an incident response team that is adequately resourced and trained?		
		Are incidents classified according to their severity and impact on the organization?		
		Are lessons from incidents reviewed and used to improve incident management?		
		Is there a post-incident review process to assess the effectiveness of the organization's response?		
		Are the results of incident reviews used to improve the organization's security posture?		
		Are there procedures for evidence collection and forensics?		

Assessment Category	Assessment Sub-Category	Assessment Items	Status	Findings
Business Continuity Management	Information Security Aspects of Business Continuity	Are information security aspects taken into account in the organization's business continuity management process?		
		Are there business continuity plans that address the loss of information or processing capabilities?		
		Are the business continuity plans regularly tested and updated?		
		Are the organization's critical business processes identified, with relevant security requirements considered?		
		Are there backups and redundancy strategies in place to ensure the availability of critical information and systems?		
		Are there measures to deal with the loss of third-party services or suppliers?		
		Is there a training and awareness program in place for business continuity plans?		
		Is there a clear understanding of which staff roles and responsibilities are crucial in the case of a disaster?		
	Redundancies	Are there redundancy strategies in place to ensure availability of information and assets?		
		Are these strategies regularly tested and updated?		
		Are there redundant systems in place for critical information systems?		
		Are there strategies in place to ensure data redundancy?		
		Are there backups of critical business information and systems?		
		Are there fail-over mechanisms in place to ensure service continuity in case of a system failure?		
		Are there plans in place to deal with the loss of third-party services or suppliers?		
		Are all redundancy systems protected and secured at the same level as the primary systems?		
Compliance	Compliance with Legal Requirements	Are all identified legal, statutory, regulatory and contractual requirements related to information security understood and documented?		
		Are there processes in place to stay informed about changes in these requirements?		
		Are there controls in place to ensure compliance with these requirements?		
		Are there regular audits and reviews to ensure compliance?		
		Is there a process in place for addressing non-compliance and making necessary improvements?		
		Are there procedures for preserving organizational records in compliance with requirements?		
		Are there processes for ensuring the protection of records, including privacy and intellectual property rights?		
		Are there procedures to comply with the secure disposal requirements defined by laws, regulations, and contracts?		
	Compliance with Security Policies and Standards	Are there regular reviews and audits to ensure compliance with organizational security policies and standards?		
		Are all deviations from security policies and standards recorded and addressed?		
		Is there a process in place for updating and improving security policies and standards based on audit findings?		
		Are all employees and third parties aware of the security policies and their obligation to comply with them?		
		Is there a process in place for addressing non-compliance by employees, contractors, and third-party users?		
		Are there guidelines in place to ensure the secure design and development of in-house developed systems?		
		Are information systems regularly checked for compliance with security policies and standards?		
		Are the security implications of changing the business processes considered and addressed?		
	Technical Compliance Checking	Are there regular technical compliance checks of information systems?		
		Are there regular checks to ensure the use of correctly licensed software?		
		Are information systems checked for compliance with security implementation standards?		
		Are there regular vulnerability assessments or penetration tests of systems and networks?		
		Is there a process in place for addressing non-compliance and vulnerabilities found during technical compliance checks?		
		Are there checks on systems to ensure that software patches are up to date?		
		Are there checks on systems to detect the presence of unauthorized software?		