ISO/IEC 27001 CHECKLIST

FRAMEWORK

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
1	4.1: Has the organization established a process to identify and evaluate both external and internal factors that are relevant to its purpose and impact its ability to achieve the intended outcomes of its Information Security Management System (ISMS)? **Process:** Conduct SWOT or PESTLE analysis during management review meetings. **Evidence:** SWOT analysis reports, meeting minutes, risk and opportunity registers.		
2	4.2: Has the organization identified relevant interested parties, assessed their associated requirements, and determined which of these requirements will be addressed by the Information Security Management System (ISMS)? **Process:** Identify stakeholders and their needs through surveys, interviews, or meetings. **Evidence:** Stakeholder mapping, documented requirements, communication records.		
3	4.3: Has the organization defined the boundaries and applicability of its Information Security Management System (ISMS) to establish its scope, considering external and internal issues, relevant requirements, and interfaces/dependencies with other organizations' activities? **Process:** Define the boundaries of the ISMS, considering dependencies and interfaces.		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
	Evidence: ISMS scope document, boundary diagrams, interface agreements.		
4	4.4: Has the organization created, implemented, maintained, and continuously improved an Information Security Management System (ISMS), encompassing the necessary processes and their interactions? **Process:** Develop and integrate ISMS processes with operational workflows. **Evidence:** ISMS manual, process interaction flowcharts, improvement plans.		
5	5.1: Has the organization's top management demonstrated leadership and commitment to the ISMS by establishing aligned information security policies and objectives, integrating ISMS requirements into processes, ensuring resource availability, communicating importance, ensuring outcomes, directing support, promoting continual improvement, and aiding other relevant management roles in demonstrating leadership? **Process:** Conduct leadership meetings to define and communicate ISMS priorities. **Evidence:** Meeting minutes, policy statements, resource allocation records.		
6	5.2: Has the organization's top management established an information security policy that is suitable for the organization's purposes, encompasses information security objectives or provides a framework for setting them, includes a commitment to fulfill applicable information security requirements, and commits to the continual		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
	improvement of the Information Security Management System (ISMS)? Additionally, is the information security policy documented, communicated within the organization, and made available to interested parties as deemed appropriate? **Process:** Draft, approve, and communicate the policy to all employees and stakeholders. **Evidence:** Approved policy document, training records, communication logs.		
7	5.3: Has the organization's top management assigned and communicated responsibilities and authorities for roles relevant to information security, including ensuring ISMS conformity to standards and reporting on its performance to top management? **Process:** Assign and document roles for ISMS responsibilities. **Evidence:** Organizational charts, job descriptions, responsibility matrices.		
8	6.1 (6.1.1): Has the organization considered relevant issues and requirements, identified, and addressed risks and opportunities, and integrated actions into ISMS processes to ensure intended outcomes, prevent undesired effects, and achieve continual improvement during the planning of its ISMS? Additionally, is the organization evaluating the effectiveness of these actions? **Process:** Risk assessment workshops and opportunity identification. **Evidence:** Risk assessment reports, action plans, effectiveness evaluations.		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
9	6.1 (6.1.2): Has the organization established and implemented an information security risk assessment process that defines criteria, ensures consistency, identifies, and analyzes risks associated with information loss, evaluates those risks against established criteria, and prioritizes them for risk treatment? **Process:** Establish criteria for risk assessment and conduct periodic reviews. **Evidence:** Risk registers, evaluation criteria, risk treatment priorities.		
10	6.1 (6.1.3): Has the organization established and implemented an information security risk treatment process that involves selecting suitable risk treatment options based on risk assessment results, determining necessary controls, comparing them with Annex A controls, producing a Statement of Applicability with justifications for inclusion/exclusion and implementation status, formulating a risk treatment plan, and obtaining risk owners' approval for the plan and acceptance of residual information security risks? **Process:** Develop a risk treatment plan and align it with Annex A controls. **Evidence:** Statement of Applicability (SoA), risk treatment plans, approval records.		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
11	6.2: Has the organization established information security objectives at relevant functions and levels, ensuring they are consistent with the information security policy, measurable (if practicable), aligned with applicable requirements, and monitored, communicated, and updated as appropriate, with retention of documented information? Additionally, when planning to achieve these objectives, has the organization determined the actions, resources, responsibilities, timeline, and evaluation methods? **Process:** Set objectives and align them with the ISMS policy. **Evidence:** Documented objectives, action plans, monitoring reports.		
12	6.3: Has the organization, when identifying the need for changes to the ISMS, carried out the implementation of these changes in a planned manner? **Process:** Implement a formal change management process. **Evidence:** Change logs, approval records, implementation plans.		
13	7.1: Has the organization determined and provided the necessary resources for the establishment, implementation, maintenance, and continual improvement of the Information Security Management System (ISMS)? **Process:** Resource planning and allocation during budgeting cycles. **Evidence:** Budget records, resource allocation logs, equipment lists.		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
14	7.2: Has the organization determined and ensured the necessary competence of individuals affecting its information security performance, taking actions as needed to acquire competence, evaluating the effectiveness of these actions, and retaining documented information as evidence of competence? **Process:** Conduct training needs analysis and provide relevant training. **Evidence:** Training records, competency evaluation results, certifications.		
15	7.3: Has the organization informed individuals working under its control about the information security policy, their contribution to ISMS effectiveness, and the consequences of non-conformance with ISMS requirements? **Process:** Conduct awareness sessions on ISMS policies and employee roles. **Evidence:** Attendance records, training materials, feedback forms.		
16	7.4: Has the organization assessed the need for internal and external communications relevant to the ISMS, specifying what to communicate, when to communicate, with whom to communicate, and how to communicate? **Process:** Develop a communication plan for internal and external information flow. **Evidence:** Communication plans, logs of information sharing, email records.		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
17	7.5 (7.5.1): Has the organization ensured that its ISMS encompasses documented information required by relevant standards and determined by the organization as necessary for the effectiveness of the ISMS? **Process:** Manage documents through a version-controlled system. **Evidence:** Document management system logs, approval records, revision histories.		
18	7.5 (7.5.2): When creating and updating documented information, has the organization ensured appropriate identification and description, including title, date, author, or reference number; determined suitable format such as language and software version, media like paper or electronic; and undergone a review and approval process for suitability and adequacy? **Process:** Manage documents through a version-controlled system. **Evidence:** Document management system logs, approval records, revision histories.		
19	7.5 (7.5.3): Has the organization controlled documented information required by the ISMS and the standard to ensure its availability and suitability for use when and where needed, as well as to provide adequate protection against issues such as loss of confidentiality, improper use, or loss of integrity? Additionally, has the organization addressed distribution, access, retrieval, use, storage, preservation (including legibility), changes (e.g., version		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
	control), retention, and disposition activities, as applicable? Moreover, has documented information of external origin deemed necessary for the planning and operation of the ISMS been appropriately identified and controlled? **Process:** Manage documents through a version-controlled system. **Evidence:** Document management system logs, approval records, revision histories.		
20	8.1: Has the organization planned, implemented, and controlled processes to meet requirements and execute actions determined in Clause 6 by establishing process criteria and implementing process controls in accordance with the established criteria? **Process:** Implement controls to achieve ISMS objectives. **Evidence:** Process criteria, monitoring records, control logs.		
21	8.2: Has the organization conducted information security risk assessments at planned intervals or when significant changes are proposed or occur, considering the criteria established in 6.1.2 a)? **Process:** Conduct periodic risk assessments or when significant changes occur. **Evidence:** Assessment reports, updated risk registers, evaluation criteria.		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
22	8.3: Has the organization executed the information security risk treatment plan as required? **Process:** Execute risk treatment plans and verify their effectiveness. **Evidence:** Implementation logs, residual risk approvals, performance metrics.		
23	9.1: Has the organization determined what needs to be monitored and measured, including information security processes and controls? Additionally, has the organization selected methods for monitoring and measurement that ensure valid, comparable, and reproducible results? Moreover, has the organization specified when and who shall perform the monitoring, and established criteria for the analysis and evaluation of results, while assigning responsibilities for these activities? **Process:** Establish a monitoring framework for ISMS performance. **Evidence:** Monitoring records, KPIs, analysis reports.		
24	9.2 (9.2.1): Has the organization conducted internal audits at planned intervals to assess whether the ISMS conforms to both the organization's own requirements and the standard's requirements, and to evaluate the effective implementation and maintenance of the ISMS? **Process:** Develop and execute an audit schedule. **Evidence:** Audit schedules, non-conformance reports, corrective action plans.		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
25	9.2 (9.2.2): Has the organization planned, established, implemented, and maintained an audit programme, considering process importance and previous audit results? Additionally, has the organization defined criteria and scope, selected auditors for objectivity, and ensured the reporting of audit results to relevant management? **Process:** Develop and execute an audit schedule. **Evidence:** Audit schedules, non-conformance reports, corrective action plans.		
26	9.3 (9.3.1): Has top management reviewed the organization's ISMS at planned intervals to ensure its ongoing suitability, adequacy, and effectiveness? **Process:** Conduct regular management reviews. **Evidence:** Review meeting minutes, decision logs, improvement action plans.		
27	9.3 (9.3.2 & 9.3.3): In the management review process, has the organization considered the status of previous actions, changes in relevant external and internal issues, shifts in the needs and expectations of interested parties, feedback on information security performance, input from interested parties, results of risk assessment, and the status of the risk treatment plan, as well as opportunities for continual improvement? **Process:** Conduct regular management reviews. **Evidence:** Review meeting minutes, decision logs, improvement action plans.		

NO	REQUIREMENT	STATUS/DESCRIPTION	REFERENCE
28	10.1: Has the organization demonstrated a commitment to the continual improvement of the suitability, adequacy, and effectiveness of the Information Security Management System (ISMS)? **Process:** Identify opportunities for improvement and implement changes. **Evidence:** Improvement logs, action plans, effectiveness reviews.		
29	10.2: Has the organization, when a nonconformity occurs, reacted by taking action to control and correct it? Additionally, has the organization addressed the consequences, evaluated the need for action to eliminate causes and prevent recurrence, implemented necessary actions, reviewed the effectiveness of corrective measures, and made changes to the ISMS if deemed necessary, ensuring that corrective actions are appropriate to the effects of the encountered nonconformities? **Process:** Investigate root causes of nonconformities and implement corrective actions. **Evidence:** Nonconformance reports, corrective action plans, verification records.		

Organizational Controls

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
1	5.1 Policies for Information Security: Are information security policies defined, approved, communicated, and periodically reviewed? **Process:** Develop overarching and topic-specific policies aligning with legal, regulatory, and organizational needs. **Evidence:** Approved policy documents, communication records, review logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
2	5.2 Information Security Roles and Responsibilities: Are roles and responsibilities for information security defined and allocated? **Process:** Clearly define roles, assign responsibilities, and ensure personnel understand their obligations. **Evidence:** Role descriptions, organizational charts, acknowledgment forms.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
3	5.3 Segregation of Duties: Are conflicting responsibilities segregated to reduce risks? **Process:** Identify potential conflicts in duties and establish segregation with compensating controls if necessary. **Evidence:** Segregation policy, access control logs, audit reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
4	5.4 Management Responsibilities: Does management ensure personnel understand and fulfill their information security responsibilities? **Process:** Assign and communicate responsibilities, monitor compliance, and provide necessary resources.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
	Evidence: Training records, management reviews, feedback from employees.		
5	5.5 Contact with Authorities: Are procedures in place for contacting authorities during information security incidents? **Process:** Maintain a list of relevant authorities and define escalation protocols for incidents. **Evidence:** Incident response plan, contact list, communication logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
6	5.6 Contact with Special Interest Groups: Does the organization maintain contact with special interest groups to stay updated on security developments? **Process:** Engage with professional forums or groups for sharing security updates. **Evidence:** Membership records, meeting minutes, correspondence logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
7	5.7 Threat Intelligence: Is threat intelligence collected, analyzed, and used to inform security measures? **Process:** Gather and analyze data on security threats to mitigate risks effectively. **Evidence:** Threat intelligence reports, risk assessments, logs of updates to security controls.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
8	5.8 Information Security in Project Management: Is information security integrated into project management processes? **Process:** Address information security risks during all project stages. **Evidence:** Project management plans, risk assessments, security requirement documentation.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
9	5.9 Inventory of Information and Other Associated Assets: Is there a maintained inventory of information and other assets, including ownership? **Process:** Document and manage assets to ensure proper classification and protection. **Evidence:** Asset inventory records, classification reports, ownership assignment documentation.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
10	5.10 Acceptable Use of Information and Other Associated Assets: Are rules for acceptable use of information and assets documented and communicated? **Process:** Establish and enforce acceptable use policies aligned with security needs. **Evidence:** Acceptable use policies, user acknowledgment records, incident logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
11	5.11 Return of Assets: Are procedures in place to ensure return of assets upon employment or contract termination? **Process:** Recover organizational assets securely during offboarding. **Evidence:** Offboarding checklists, asset recovery records, termination procedures.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
12	5.12 Classification of Information: Is information classified based on confidentiality, integrity, and availability requirements? **Process:** Implement a classification scheme to protect information based on its sensitivity. **Evidence:** Classification policies, classification reports, access control logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
13	5.13 Labelling of Information: Are labeling procedures in place to reflect the information classification scheme? **Process:** Ensure all classified information is labeled appropriately for secure handling. **Evidence:** Labeling policies, labeled documents, metadata configurations.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
14	5.14 Information Transfer: Are secure procedures in place for the transfer of information within and outside the organization? **Process:** Establish controls to protect information during all types of transfers. **Evidence:** Transfer policies, agreements, logs of secure information transfers.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
15	5.15 Access Control: Are access control policies implemented to restrict access based on business needs? **Process:** Define and enforce access policies to restrict physical and logical access to authorized individuals. **Evidence:** Access control policies, access logs, and review records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
16	5.16 Identity Management: Are identity management processes implemented to ensure proper access control? **Process:** Establish processes for creating, maintaining, and deactivating identities in a secure manner. **Evidence:** Identity lifecycle policies, user access logs, and audit reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
17	5.17 Authentication Information: Are authentication mechanisms securely managed to prevent unauthorized access? **Process:** Implement strong authentication methods and protect credentials with encryption. **Evidence:** Authentication policies, password storage configurations, MFA logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
18	5.18 Access Rights: Are access rights regularly reviewed and updated based on roles and responsibilities? **Process:** Define, assign, and periodically review access rights to align with organizational needs. **Evidence:** Role-based access control policies, access reviews, and change logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
19	5.19 Information Security in Supplier Relationships: Are supplier relationships managed to ensure compliance with security requirements? **Process:** Assess and monitor suppliers against defined security criteria. **Evidence:** Supplier agreements, performance reviews, and compliance audit reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
20	5.20 Addressing Information Security in Supplier Agreements: Are security requirements clearly defined in supplier contracts? **Process:** Include specific security clauses and expectations in supplier agreements. **Evidence:** Supplier contracts with security clauses, contract review records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
21	5.21 Managing Information Security in the ICT Supply Chain: Is the ICT supply chain monitored for security risks and compliance? **Process:** Define and enforce requirements for ICT suppliers to manage supply chain risks. **Evidence:** Supplier assessments, risk management plans, compliance records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
22	5.22 Monitoring, Review, and Change Management of Supplier Services: Are supplier services monitored for security performance and compliance? **Process**: Establish review processes to monitor and evaluate supplier service performance. **Evidence:** Monitoring reports, supplier meeting records, and change logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
23	5.23 Information Security for Use of Cloud Services: Are cloud services evaluated and managed for information security risks? **Process:** Assess cloud providers and continuously monitor their compliance with security requirements. **Evidence:** Cloud service agreements, risk assessment reports, and security monitoring logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
24	5.24 Incident Management Planning and Preparation: Are incident management plans developed and tested regularly? **Process:** Develop, document, and periodically test incident response plans. **Evidence:** Incident response plans, test results, and improvement logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
25	5.25 Assessment and Decision on Security Events: Are security events assessed, and decisions made to mitigate potential incidents? **Process:** Establish processes to evaluate security events and determine appropriate responses. **Evidence:** Event assessment logs, decision records, and response plans.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
26	5.26 Response to Information Security Incidents: Are incidents managed effectively to minimize impact? **Process:** Define response procedures, roles, and escalation paths for handling incidents. **Evidence:** Incident logs, response team training records, and post-incident reviews.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
27	5.27 Learning from Security Incidents: Are lessons from incidents documented and used to improve security measures? **Process:** Conduct post-incident analyses and update controls based on findings. **Evidence:** Post-incident review reports, updated procedures, and training materials.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
28	5.28 Collection of Evidence: Is evidence collection during incidents conducted securely and in compliance with laws? **Process:** Develop procedures to securely collect, preserve, and document evidence during incidents. **Evidence:** Evidence collection logs, chain of custody records, and incident investigation reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
29	5.29 Information Security During Disruption: Are measures in place to maintain information security during disruptions? **Process:** Implement and test contingency plans to manage disruptions. **Evidence:** Contingency plans, test results, and incident management logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
30	5.30 ICT Readiness for Business Continuity: Are ICT systems prepared to support business continuity plans? **Process:** Establish and regularly test ICT systems to ensure availability during disruptions. **Evidence:** Business continuity test reports, system readiness assessments, and recovery logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
31	5.31 Legal, Statutory, Regulatory, and Contractual Requirements: Are applicable legal and regulatory requirements documented and monitored for compliance? **Process:** Identify, document, and regularly review compliance with all applicable requirements. **Evidence:** Compliance records, legal registry, and audit results.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
32	5.32 Intellectual Property Rights: Are intellectual property rights managed to prevent violations and ensure compliance? **Process:** Implement policies for managing and protecting intellectual property. **Evidence:** Intellectual property policy, licensing records, and compliance audit logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
33	5.33 Protection of Records: Are records managed securely to prevent loss, destruction, or unauthorized access? **Process:** Implement access controls, retention schedules, and secure storage for records. **Evidence:** Record management policies, access logs, and backup reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
34	5.34 Privacy and Protection of PII: Are processes in place to protect personal identifiable information (PII) in compliance with regulations? **Process:** Implement data protection measures and privacy impact assessments. **Evidence:** PII protection policies, DPIA reports, and incident logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
35	5.35 Independent Review of Information Security: Are independent reviews conducted to assess information security effectiveness? **Process:** Arrange periodic independent audits of the ISMS and associated controls. **Evidence:** Audit plans, reports, and corrective action records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
36	5.36 Compliance with Policies, Rules, and Standards: Are compliance with internal policies, rules, and standards regularly monitored? **Process:** Conduct periodic reviews to verify compliance with organizational standards and requirements. **Evidence:** Compliance reports, policy review records, and non-conformance logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
37	5.37 Documented Operating Procedures: Are operating procedures documented and maintained to ensure secure and efficient operations? **Process:** Define, document, and regularly update procedures for critical operations. **Evidence:** Operating procedure documents, change logs, and training records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

People Controls

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
1	6.1 Screening: Are background checks conducted on personnel prior to employment? **Process:** Screen candidates as per applicable laws and the sensitivity of their role. **Evidence:** Screening records, policy documents, vendor contracts for screening services.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
2	6.2 Terms and Conditions of Employment: Do employment contracts include information security requirements? **Process:** Incorporate confidentiality agreements, security clauses, and termination conditions. **Evidence:** Signed contracts, HR forms and records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
3	6.3 Information Security Awareness, Education, and Training: Are personnel provided with regular information security awareness and training? **Process:** Develop and implement training programs to ensure awareness of security responsibilities.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
	Evidence: Training plans, attendance records, feedback.		
4	6.4 Disciplinary Process: Is there a disciplinary process for addressing breaches of information security policies? **Process:** Define and enforce consequences for non-compliance with security policies. **Evidence:** Disciplinary procedures, incident logs, records of actions taken.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
5	6.5 Responsibilities After Termination or Change of Employment: Are responsibilities for protecting organizational information clearly defined after employment termination or change? **Process:** Ensure departing employees or role changers return assets and maintain confidentiality. **Evidence:** Exit interview records, confidentiality agreements, asset return logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
6	6.6 Confidentiality or Non-Disclosure Agreements: Are confidentiality or non-disclosure agreements in place for employees and external parties? **Process:** Establish agreements to protect sensitive information during and after employment. **Evidence:** Signed agreements, policy documents, compliance audit results.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
7	6.7 Remote Working: Are secure practices implemented for remote working to protect information security? **Process:** Define and enforce security measures for remote work environments.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
	Evidence: Remote work policies, VPN usage logs, training records on remote work security.		
8	6.8 Information Security Event Reporting: Are procedures in place for personnel to report information security events? **Process:** Create clear channels for event reporting and ensure timely response. **Evidence:** Incident reporting forms, event logs, communication records with relevant stakeholders.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

Physical Controls

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
1	7.1 Physical Security Perimeters: Are physical security perimeters established to protect information and assets? **Process:** Define and implement secured areas with appropriate access controls. **Evidence:** Floor plans, access logs, security assessments.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
2	7.2 Physical Entry: Are physical entry controls implemented to restrict access to authorized personnel? **Process:** Use mechanisms like badges, guards, or biometric controls to manage access. **Evidence:** Access logs, visitor records, system configurations.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
3	7.3 Securing Offices, Rooms, and Facilities: Are offices, rooms, and facilities secured to prevent unauthorized access? **Process:** Implement locking systems, surveillance, and visitor management procedures.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
	Evidence: Surveillance logs, security system records, visitor sign-in sheets.		
4	7.4 Physical Security Monitoring: Is physical security monitoring in place to detect and respond to unauthorized access attempts? **Process:** Install and maintain surveillance systems, alarms, and monitoring protocols. **Evidence:** CCTV footage, maintenance logs, incident reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
5	7.5 Protecting Against Physical and Environmental Threats: Are physical and environmental threats like fire, flood, and natural disasters mitigated through appropriate controls? **Process:** Implement measures such as fire detection systems, climate controls, and disaster planning. **Evidence:** Disaster recovery plans, maintenance records, risk assessment reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
6	7.6 Working in Secure Areas: Are secure areas designated, and are personnel trained to work securely within them? **Process:** Define secure zones, restrict access, and establish protocols for work in these areas. **Evidence:** Access control logs, training records, secure area policies.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
7	7.7 Clear Desk and Clear Screen: Are clear desk and clear screen policies enforced to protect sensitive information? **Process:** Mandate secure storage of sensitive documents and lock screens when unattended.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
	Evidence: Policy documents, inspection logs, awareness training records.		
8	7.8 Equipment Siting and Protection: Is equipment sited and protected to reduce risks of unauthorized access, damage, or theft? **Process:** Position equipment securely and protect it from environmental and physical threats. **Evidence:** Equipment placement guidelines, inspection records, incident reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
9	7.9 Security of Assets Off-Premises: Are organizational assets used off-premises adequately secured? **Process:** Define controls for securing assets used in remote or mobile settings. **Evidence:** Asset usage policies, employee acknowledgment records, incident logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
10	7.10 Storage Media: Are storage media secured and handled to prevent unauthorized access, loss, or damage? **Process:** Implement secure storage, transfer, and disposal procedures for media. **Evidence:** Media handling policies, disposal records, access control logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
11	7.11 Supporting Utilities: Are supporting utilities like power and cooling systems maintained to ensure availability and reliability? **Process:** Regularly inspect and maintain utilities that support information processing facilities.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
	Evidence: Maintenance logs, utility service agreements, incident reports		
12	7.12 Cabling Security: Is cabling for data and power secured to protect against interception and damage? **Process:** Protect cables by using secure conduits, shielding, and regular inspections. **Evidence:** Cable layout plans, inspection reports, incident logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
13	7.13 Equipment Maintenance: Is equipment maintained securely to ensure functionality and information protection? **Process:** Establish procedures for equipment servicing and ensure service providers follow security protocols. **Evidence:** Maintenance logs, service provider contracts, inspection records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
14	7.14 Secure Disposal or Re-Use of Equipment: Are secure procedures in place for disposing or reusing equipment containing sensitive data? **Process:** Erase data and decommission equipment securely before disposal or reuse. **Evidence:** Disposal logs, destruction certificates, inspection records of reused equipment.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

Technological Controls

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
1	8.1 User Endpoint Devices: Are endpoint devices managed and secured against unauthorized access? **Process:** Implement endpoint security solutions and enforce policies on device usage. **Evidence:** Endpoint security configurations, incident logs, training records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
2	8.2 Privileged Access Rights: Are privileged access rights controlled and monitored? **Process:** Assign and manage privileged access on a need-to-know basis and audit periodically. **Evidence:** Access control policies, audit reports, user access reviews.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
3	8.3 Information Access Restriction: Are restrictions on information access enforced based on classification and business needs? **Process:** Implement controls to limit access to information and enforce policies consistently. **Evidence:** Access control policies, user access logs, classification reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
4	8.4 Access to Source Code: Is access to source code restricted and monitored to prevent unauthorized changes? **Process:** Secure source code repositories with appropriate access controls and monitor for changes. **Evidence:** Source code access logs, repository audit reports, policy documents.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
5	8.5 Secure Authentication: Are secure authentication methods implemented to protect access to systems? **Process:** Enforce strong authentication mechanisms like multi-factor authentication (MFA). **Evidence:** Authentication logs, MFA configurations, training records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
6	8.6 Capacity Management: Is capacity managed to ensure system performance and availability under normal and peak conditions? **Process:** Monitor and optimize system performance regularly to prevent disruptions. **Evidence:** Capacity planning reports, system performance logs, monitoring tool configurations.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
7	8.7 Protection Against Malware: Are measures in place to prevent, detect, and respond to malware incidents? **Process:** Deploy and update anti-malware tools and conduct regular scans. **Evidence:** Anti-malware logs, policy documents, incident response records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
8	8.8 Management of Technical Vulnerabilities: Are technical vulnerabilities identified, assessed, and remediated promptly? **Process:** Regularly scan systems, prioritize vulnerabilities, and implement fixes. **Evidence:** Vulnerability assessment reports, patching logs, remediation plans.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
9	8.9 Configuration Management: Are secure configuration settings maintained and monitored for all systems? **Process:** Establish and enforce baseline configurations for hardware and software. **Evidence:** Configuration baselines, audit reports, change logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
10	8.10 Information Deletion: Are secure methods implemented to delete information when no longer required? **Process:** Use tools and methods for secure deletion of sensitive data from storage devices. **Evidence:** Deletion policies, logs of deletion activities, verification records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
11	8.11 Data Masking: Is data masking used to protect sensitive information in non-production environments? **Process:** Implement masking techniques to obfuscate sensitive data where applicable. **Evidence:** Data masking policies, implementation reports, testing logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
12	8.12 Data Leakage Prevention: Are measures in place to prevent unauthorized exfiltration of data? **Process:** Deploy data loss prevention (DLP) tools and monitor for suspicious activities. **Evidence:** DLP tool configurations, incident reports, monitoring logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
13	8.13 Information Backup: Are backups performed regularly and tested for recovery to ensure availability of critical data? **Process:** Establish a backup policy with regular testing of recovery processes. **Evidence:** Backup schedules, recovery testing logs, backup policies.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
14	8.14 Redundancy of Information Processing Facilities: Are redundant facilities implemented to ensure availability during disruptions? **Process:** Deploy redundant systems and networks to support critical processes. **Evidence:** Disaster recovery plans, redundancy configurations, system testing reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
15	8.15 Logging: Are logging mechanisms implemented to monitor and track security events? **Process:** Ensure secure logging of critical events with monitoring for anomalies. **Evidence:** Log files, monitoring reports, incident investigation records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
16	8.16 Monitoring Activities: Are monitoring activities conducted to detect security incidents promptly? **Process:** Use tools to monitor system activity and generate alerts for anomalies. **Evidence:** Monitoring configurations, incident logs, response plans.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
17	8.17 Clock Synchronization: Are system clocks synchronized to ensure accurate logging and event correlation? **Process:** Synchronize clocks across systems using protocols like NTP. **Evidence:** NTP configurations, audit logs, monitoring reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
18	8.18 Use of Privileged Utility Programs: Are privileged utility programs restricted and monitored to prevent misuse? **Process:** Limit access to and monitor the use of privileged utilities. **Evidence:** Access control policies, usage logs, audit records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
19	8.19 Installation of Software on Operational Systems: Is software installation on operational systems controlled and monitored? **Process:** Implement controls to authorize and document software installations. **Evidence:** Software installation policies, authorization logs, change management records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
20	8.20 Network Security: Are network security controls implemented to protect communication channels? **Process:** Deploy firewalls, IDS/IPS, and encryption for securing networks. **Evidence:** Network security configurations, monitoring logs, incident response reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
21	8.21 Security of Network Services: Are network services secured to ensure availability, confidentiality, and integrity? **Process:** Ensure providers and services comply with security requirements. **Evidence:** Service agreements, monitoring logs, incident response reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
22	8.22 Segregation of Networks: Are networks segregated to minimize risks and protect sensitive information? **Process:** Implement VLANs and other segmentation techniques to limit traffic between networks. **Evidence:** Network segmentation diagrams, access control policies, monitoring logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
23	8.23 Web Filtering: Is web filtering implemented to prevent access to malicious or inappropriate websites? **Process:** Deploy and configure web filtering solutions. **Evidence:** Web filtering policies, usage logs, incident reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
24	8.24 Use of Cryptography: Is cryptography used to protect sensitive data in transit and at rest? **Process:** Implement encryption protocols and manage keys securely. **Evidence:** Encryption policies, key management records, testing reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
25	8.25 Secure Development Life Cycle: Is a secure development life cycle process implemented to minimize software vulnerabilities? **Process:** Integrate security into all phases of the development life cycle. **Evidence:** Development policies, secure coding guidelines, testing records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
26	8.26 Application Security Requirements: Are security requirements identified and implemented for all applications? **Process:** Establish and enforce security requirements in development and procurement processes. **Evidence:** Application security requirements, testing reports, deployment logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
27	8.27 Secure System Architecture and Engineering Principles: Are secure architecture and engineering principles applied to all system designs? **Process:** Apply security principles to system design and maintenance processes. **Evidence:** Architecture diagrams, design review records, testing reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
28	8.28 Secure Coding: Are secure coding practices enforced during application development? **Process:** Provide training and enforce coding standards for developers. **Evidence:** Secure coding guidelines, developer training records, code review reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
29	8.29 Security Testing in Development and Acceptance: Are security tests conducted during development and acceptance stages? **Process:** Perform security testing regularly and address findings promptly. **Evidence:** Testing reports, remediation logs, testing tools configurations.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
30	8.30 Outsourced Development: Are outsourced development projects monitored for compliance with security requirements? **Process:** Include security requirements in contracts and perform audits on outsourced work. **Evidence:** Contracts, audit reports, testing records.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
31	8.31 Separation of Development, Test, and Production Environments: Are development, test, and production environments separated to prevent risks? **Process:** Maintain strict controls to isolate these environments. **Evidence:** Environment diagrams, access control policies, change logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
32	8.32 Change Management: Is a change management process in place to ensure changes are documented, tested, and approved? **Process:** Implement a formal process for managing changes to systems and applications. **Evidence:** Change management records, approval logs, testing reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	

NO	CONTROL	STATUS/DESCRIPTION	REFERENCE
33	8.33 Test Information: Is test information protected to prevent unauthorized access or disclosure? **Process:** Mask or anonymize sensitive data in test environments. **Evidence:** Test environment policies, data masking records, audit logs.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	
34	8.34 Protection of Information Systems During Audit Testing: Are information systems protected from compromise during audit testing? **Process:** Implement controls to prevent disruptions or leaks during audits. **Evidence:** Audit plans, test logs, incident reports.	Mark the box that applies: ☐ Applicable ☐ Not Applicable	