Azpirant
TECHNOLOGIES

ISO/IEC 27001:2022
Security Controls Implementation
✓ Checklist

Annex A (Normative)

Annex A.5: Organizational Controls

A.5.1: Policies for Information Security

Requirement	Status (Yes / No / Partially / N/A)	Comments/ Evidence	Remarks
Has the organization defined, approved, and communicated a comprehensive information security policy and topic-specific policies to relevant personnel and stakeholders?			
Are these policies reviewed regularly and updated when significant changes occur?			

A.5.2: Information Security Roles and Responsibilities

Are roles and responsibilities for information security clearly defined, allocated, and aligned with organizational needs?			

A.5.3: Segregation of Duties

Are conflicting duties or responsibilities appropriately segregated to reduce risk and avoid misuse?			

A.5.4: Management Responsibilities

Do managers actively require personnel to follow security policies and procedures in daily operations?			

A.5.5: Contact with Authorities

Are procedures in place for contacting authorities during information security incidents?	Maintain a list of relevant authorities and define escalation protocols for incidents.	Incident response plan, contact list, communication logs.	

A.5.6: Contact with Special Interest Groups

Does the organization maintain active contact with industry groups, security forums, or professional associations for knowledge exchange?			

A.5.7: Threat Intelligence

Is the organization collecting, analyzing, and acting on threat intelligence relevant to its risk profile?			

A.5.8: Information Security in Project Management

Is information security integrated into all phases of project management across the organization?			

A.5.9: Inventory of Information and Other Assets

Is there a documented inventory of information and associated assets, including ownership assignment?			

A.5.10: Acceptable Use of Assets

Are rules for the acceptable use and protection of assets defined, documented, and enforced?			

A.5.11: Return of Assets

Is there a formal process to ensure return of assets upon employment termination or role change?			

A.5.12: Classification of Information

Has the organization defined and applied a classification scheme for information based on confidentiality, integrity, availability, and stakeholder requirements?			

A.5.13: Labelling of Information

Are procedures for labelling information in line with the classification scheme developed and implemented?			

A.5.14: Information Transfer

Are there controls and procedures for transferring information securely between parties and systems, whether internal or external?			

A.5.15: Access Control

Are physical and logical access rules documented and implemented according to business and security requirements?			

A.5.16: Identity Management

Is the full lifecycle of user identities managed securely, including creation, use, and deactivation?			

A.5.17: Authentication Information

Are processes in place to manage, distribute, and secure authentication credentials, such as passwords or tokens?			

A.5.18: Access Rights

Are access rights granted, reviewed, modified, and revoked according to defined access control policies?			

A.5.19: Information Security in Supplier Relationships

Are security risks in supplier-provided products/services identified and managed through formal processes?			

A.5.20: Security in Supplier Agreements

Do supplier agreements include specific clauses to address information security requirements?			

A.5.21: ICT Supply Chain Security

Are controls implemented to manage security risks in the ICT supply chain, including service providers and third-party vendors?			

A.5.22: Monitoring and Review of Supplier Services

Are supplier services regularly reviewed, monitored, and assessed for information security compliance?			

A.5.23: Information Security for Cloud Services

Are there documented controls for the acquisition, use, and exit of cloud services, ensuring compliance with the organization's ISMS?			

A.5.24: Incident Management Planning and Preparation

Has the organization established and communicated incident response roles, plans, and procedures?			

A.5.25: Assessment and Decision on Security Events

Are information security events evaluated promptly to determine whether they should be treated as incidents?			

A.5.26: Response to Information Security Incidents

Are incident response activities carried out in accordance with documented procedures?			

A.5.27: Learning from Information Security Incidents

Is knowledge from incidents reviewed and used to strengthen ISMS controls?			

A.5.28: Collection of Evidence

Are there formal procedures for the collection and preservation of evidence related to security events?			

A.5.29: Information Security During Disruption

Are plans in place to maintain information security during business disruptions (e.g., natural disasters, cyberattacks)?			

A.5.30: ICT Readiness for Business Continuity

Are ICT systems and infrastructure prepared, tested, and maintained for continuity in line with business needs?			

A.5.31: Legal, Regulatory, and Contractual Requirements

Has the organization identified and documented all applicable legal, regulatory, and contractual obligations related to information security?			

A.5.32: Intellectual Property Rights

Are procedures in place to protect intellectual property, including copyright, trademarks, and proprietary software?			

A.5.33: Protection of Records

Are records protected from loss, destruction, unauthorized access, and falsification?			

A.5.34: Privacy and Protection of PII

Are processes in place to ensure compliance with privacy regulations and the protection of personally identifiable information (PII)?			

A.5.35: Independent Review of Information Security

Is the organization's information security program independently reviewed at planned intervals, or upon significant change?			

A.5.36: Compliance with Policies and Standards

Are compliance checks performed regularly to ensure adherence to internal policies and standards?			

A.5.37: Documented Operating Procedures

Are operational procedures documented, updated, and made available to personnel as needed?			

Annex A.6: People Controls

A.6.1: Screening

Requirement	Status (Yes / No / Partially / N/A)	Comments/ Evidence	Remarks
Are background verification checks performed on all candidates prior to employment, and periodically afterward as appropriate?			
Are these checks in line with applicable laws, ethics, job roles, and information classification levels?			

A.6.2: Terms and Conditions of Employment

Do employment contracts and agreements explicitly outline employee responsibilities related to information security?			
Are these responsibilities aligned with the organization's ISMS policies and controls?			

A.6.3: Information Security Awareness, Education, and Training

Is there a structured program to provide regular awareness and training on information security for all personnel and relevant external parties?			
Are updates provided based on policy changes, emerging threats, or incidents?			

A.6.4: Disciplinary Process

Has the organization defined and communicated a formal disciplinary process for violations of information security policies?			
Is this process consistently enforced and proportional to the severity of violations?			

A.6.5: Responsibilities After Termination or Role Change

Are post-employment or post-role change responsibilities related to information security (e.g., confidentiality, access removal) defined and communicated?			
Are exit procedures followed to revoke access, return assets, and reinforce ongoing obligations?			

A.6.6: Confidentiality or Non-Disclosure Agreements (NDAs)

Are NDAs or confidentiality agreements required and signed by employees and relevant third parties?			
Are these agreements regularly reviewed and updated to reflect organizational needs?			

A.6.7: Remote Working

Has the organization implemented controls for secure remote work, including endpoint protection, secure connectivity, and data handling practices?			
Are personnel trained and monitored to ensure secure behavior while working off-site?			

A.6.8: Information Security Event Reporting

Are personnel provided with clear procedures and tools to report suspected or observed security events in a timely manner?			
Is there a culture that encourages prompt and honest reporting without fear of retaliation?			

Annex A.7: Physical Controls

Requirement	Status (Yes / No / Partially / N/A)	Comments/ Evidence	Remarks
A.7.1: Physical Security Perimeters			
Are physical security perimeters (e.g., fences, locked doors, mantraps) defined and implemented to protect sensitive areas from unauthorized access?			
A.7.2: Physical Entry			
Are entry points to secure areas protected with appropriate access control measures (e.g., keycards, biometric systems, visitor logs)?			
A.7.3: Securing Offices, Rooms, and Facilities			
Are offices and facilities designed with security in mind, including controlled entry, minimal access to sensitive areas, and proper locking mechanisms?			
A.7.4: Physical Security Monitoring			
Are premises continuously monitored using surveillance systems, guards, or intrusion detection systems to prevent unauthorized physical access?			
A.7.5: Protection Against Physical and Environmental Threats			
Are facilities protected against natural disasters, fire, flood, power outages, and other environmental risks?			
A.7.6: Working in Secure Areas			
Are procedures established for working in secure areas, including restrictions on unauthorized activities or equipment?			
A.7.7: Clear Desk and Clear Screen Policy			
Are clear desk and clear screen policies enforced to ensure sensitive information and systems are not exposed when unattended?			

A.7.8: Equipment Siting and Protection

Is equipment placed securely to prevent unauthorized access or damage, and protected from environmental hazards?			

A.7.9: Security of Assets Off-Premises

Are organizational assets used outside the premises (e.g., laptops, USBs, phones) protected with encryption, tracking, or access controls?			

A.7.10: Storage Media

Are storage media (e.g., USBs, external drives) managed throughout their lifecycle—acquisition, usage, transport, and disposal?			

A.7.11: Supporting Utilities

Are power, HVAC, and communication utilities maintained and protected to ensure uninterrupted operation of information systems?			

A.7.12: Cabling Security

Are cables carrying power and data protected from interception, interference, or accidental damage?			

A.7.13: Equipment Maintenance

Is equipment regularly maintained and serviced to ensure secure and reliable operation?			

A.7.14: Secure Disposal or Reuse of Equipment

Are devices securely wiped or destroyed before disposal or reuse to prevent unauthorized access to residual data?			

Annex A.8: Technological Controls

A.8.1: User End Point Devices

Requirement	Status (Yes / No / Partially / N/A)	Comments/ Evidence	Remarks
Are endpoint devices (laptops, desktops, mobile devices) secured with appropriate controls, such as full disk encryption, endpoint detection and response (EDR), and screen auto-lock?			
Are security configurations standardized and maintained, including OS hardening and disabling unused ports or services?			

A.8.2: Privileged Access Rights

Are privileged accounts (e.g., admin, root) strictly limited, monitored, and documented?			
Are approvals required for granting elevated access, and are rights reviewed periodically?			

A.8.3: Information Access Restriction

Is access to data, systems, and applications restricted based on role, need-to-know, and least privilege principles?			
Are technical access controls (e.g., ACLs, firewalls, role-based access) in place and enforced?			

A.8.4: Access to Source Code

Is access to source code repositories and development environments restricted to authorized developers?			
Are write operations logged, and is version control enforced?			

A.8.5: Secure Authentication

Are multi-factor authentication (MFA) and secure password policies enforced for access to sensitive systems?			
Are authentication mechanisms aligned with risk levels, such as biometric or token-based access?			

A.8.6: Capacity Management

Are IT resources (e.g., compute, storage, bandwidth) monitored, planned, and scaled according to forecasted demand?			
Are tools in place to alert performance or capacity issues?			

A.8.7: Protection Against Malware

Are anti-malware solutions deployed, regularly updated, and centrally managed across all endpoints and servers?			
Is there user awareness training on phishing and unsafe downloads?			

A.8.8: Management of Technical Vulnerabilities

Are technical vulnerabilities identified using tools like vulnerability scanners, CVE databases, or vendor advisories?			
Are patches applied promptly, based on risk and criticality, following a formal vulnerability management process?			

A.8.9: Configuration Management

Are baseline configurations defined and enforced for hardware, software, and network devices?			
Are changes documented, approved, and tracked through a change management process?			

A.8.10: Information Deletion

Are secure deletion methods used when disposing of data on storage media (e.g., wiping, degaussing, physical destruction)?			
Are data retention policies enforced and monitored?			

A.8.11: Data Masking

Is data masking or obfuscation applied to sensitive data in non-production environments or when used by third parties?			

A.8.12: Data Leakage Prevention

Are DLP tools and controls deployed to monitor and prevent unauthorized transfer or disclosure of sensitive data (e.g., USB blocking, outbound email scanning)?			

A.8.13: Information Backup

Are automated backups scheduled for critical systems and data?			
Are backups encrypted, stored securely offsite, and tested regularly for restoration?			

A.8.14: Redundancy of Information Processing Facilities

Are redundant systems and infrastructure (e.g., clustering, load balancing, failover) implemented to meet availability requirements?			

A.8.15: Logging

Are logs generated for critical activities (e.g., login attempts, system changes, access to sensitive data)?			
Are logs protected from tampering and retained in accordance with policy?			

A.8.16: Monitoring Activities

Are real-time monitoring tools (e.g., SIEM) used to detect anomalous behavior or unauthorized activities?			
Are alerts generated and reviewed by security personnel?			

A.8.17: Clock Synchronization

Are system clocks synchronized with a secure, trusted time source (e.g., NTP server) to ensure log integrity?			

A.8.18: Use of Privileged Utility Programs

Is the use of utility programs that override security (e.g., disk editors, password reset tools) tightly controlled and logged?			

A.8.19: Installation of Software on Operational Systems

Are users restricted from installing unauthorized software on operational systems?			
Are installation processes governed by policy and require approval?			

A.8.20: Network Security

Are networks segmented and protected using firewalls, IDS/IPS, and other perimeter defenses?			
Are secure network configurations documented and regularly reviewed?			

A.8.21: Security of Network Services

Are network services (e.g., DNS, VPN, VoIP) configured with secure protocols and monitored for misuse?			
Are security expectations agreed upon in SLAs with service providers?			

A.8.22: Segregation of Networks

Are network zones logically or physically segregated (e.g., internal vs DMZ vs guest)?			
Is inter-zone communication limited and controlled through firewalls or ACLs?			

A.8.23: Web Filtering

Are web filtering solutions implemented to block access to known malicious or non-business-related websites?			

A.8.24: Use of Cryptography

Are cryptographic methods and key management practices implemented per organizational policy and compliance requirements (e.g., AES, RSA, PKI)?			

A.8.25: Secure Development Life Cycle

Are secure coding practices integrated into the software development lifecycle (SDLC)?			
Are developers trained in secure development, and are security reviews or threat modeling performed?			

A.8.26: Application Security Requirements

Are security requirements defined and documented before developing or acquiring applications?			

A.8.27: Secure System Architecture and Engineering Principles

Are secure architecture principles established and applied to all system and application design activities?			

A.8.28: Secure Coding

Are secure coding guidelines followed, including protection against OWASP Top 10 vulnerabilities?			

A.8.29: Security Testing in Development and Acceptance

Is security testing (e.g., static analysis, dynamic testing, penetration testing) conducted as part of development and before production release?			

A.8.30: Outsourced Development

Is outsourced software development monitored, reviewed, and contractually bound by security requirements?			

A.8.31: Separation of Development, Test, and Production Environments

Are development, test, and production environments logically and physically separated to avoid accidental or unauthorized access?			

A.8.32: Change Management

Are changes to systems, applications, and infrastructure approved, documented, tested, and reviewed before deployment?			

A.8.33: Test Information

Is test data sanitized and protected, especially when derived from production environments?			

A.8.34: Protection of Systems During Audit and Testing

Are audit and testing activities planned and authorized, ensuring they do not disrupt system operations or compromise data?			

READY TO ENHANCE YOUR DIGITAL RESILIENCE?

Follow us for daily tips!

Azpirantz
TECHNOLOGIES

For expert consulting and professional advice, please reach out to sales@azpirantz.com

**This content has been created and published by the Azpirantz Marketing Team and should not be considered a professional advice*