**ISO/IEC 27001:2022 READINESS CHECKLIST:**

This document serves as a comprehensive readiness tool for B2B SaaS companies preparing for ISO/IEC 27001:2022 certification. It is designed to assist internal security, compliance, DevOps, and executive teams in systematically implementing the Information Security Management System (ISMS) requirements set forth by the standard.

It outlines specific control actions, assigns responsibility, and maps each step to leading compliance frameworks including: NIST CSF, NIST SP 800 Series, ISO/IEC 27001, HIPAA, PCI DSS, GDPR, COBIT, and CCPA. Each control is broken down with clear objectives, operational requirements, and practical evidence examples to support your internal readiness program and third-party audit process.

**USAGE NOTES:**

* This is not a substitute for official ISO standards or third-party audit guidance.
* It is optimized for internal readiness, control implementation tracking, and audit preparation.
* Customization is encouraged to reflect unique organizational risk profiles and architectures.

TABLE OF CONTENTS:

[CLAUSE 4 – CONTEXT OF THE ORGANIZATION 2](#_Toc197255823)

[CLAUSE 5 – LEADERSHIP 2](#_Toc197255824)

[CLAUSE 6 – PLANNING 3](#_Toc197255825)

[CLAUSE 7 – SUPPORT 4](#_Toc197255826)

[CLAUSE 8 – OPERATION 5](#_Toc197255827)

[CLAUSE 9 – PERFORMANCE EVALUATION 5](#_Toc197255828)

[ANNEX A.5 — ORGANIZATIONAL CONTROLS 6](#_Toc197255829)

[ANNEX A.6 — PEOPLE CONTROLS 12](#_Toc197255830)

[ANNEX A.7 — PHYSICAL CONTROLS 14](#_Toc197255831)

[ANNEX A.8 — TECHNOLOGICAL CONTROLS 16](#_Toc197255832)

[FRAMEWORK REFERENCE SUMMARIES: 22](#_Toc197255833)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CLAUSE 4 – CONTEXT OF THE ORGANIZATION **Goal:** Define the business and regulatory context, interested parties, and ISMS boundaries. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 4.1 Understand the Organization and Context | * Conduct a business impact and environment analysis (SWOT, PESTLE). * Document internal/external factors affecting security (e.g., regulatory, cloud dependencies). | Compliance Lead, CISO | * Context analysis doc * Risk registers * Cloud provider terms | NIST CSF ID.AM-5, NIST SP 800-53 PM-11, COBIT APO12 |
| 4.2 Identify Interested Parties | * List stakeholders (e.g., customers, regulators, hosting providers). * Define their expectations (e.g., GDPR, uptime SLAs). | Compliance Officer, Legal | * Stakeholder register * DPA agreements * GDPR applicability review | NIST CSF ID.BE-1, HIPAA 164.308(a)(1), COBIT APO02 |
| 4.3 Define ISMS Scope | * Document which departments, tools, infrastructure, and services fall under the ISMS. * Tailor to application delivery lifecycle. | CISO, IT Manager | * ISMS scope document and diagrams * Cloud asset lists | NIST SP 800-53 PL-2, ISO 27701 Clause 5.2.1 |
| 4.4 Establish ISMS | * Formalize the ISMS. * Assign roles, define documentation structure, and establish a PDCA cycle. | CISO | * ISMS policy * Governance chart * PDCA implementation plan | COBIT EDM01, NIST CSF ID.GV-1, ISO 27001 policy register |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CLAUSE 5 – LEADERSHIP **Goal:** Establish top-level commitment, define information security policies, and assign governance responsibilities. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 5.1 Leadership & Commitment | * Ensure executives actively support the ISMS: assign authority, approve resources, and integrate security into business strategy. | CEO, CISO | * Signed ISMS charter * Exec meeting minutes * Budget approval for ISMS | NIST CSF ID.GV-1, NIST SP 800-53 PM-1, COBIT APO01 |
| 5.2 Information Security Policy | * Write and distribute a high-level InfoSec Policy that reflects the SaaS product’s confidentiality, integrity, and availability needs. | CISO, Security Manager | * Approved InfoSec policy with version history * Internal memo | NIST SP 800-53 PL-1, PCI DSS 12.1, GDPR Art. 24 |
| 5.3 Organizational Roles, Responsibilities & Authorities | * Document key ISMS roles (e.g., DPO, AppSec Lead, Risk Owner), and communicate them org-wide. | HR, CISO | * RACI matrix * Job descriptions * Onboarding materials | NIST SP 800-53 AT-1, HIPAA 164.308(a)(2), COBIT BAI09 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CLAUSE 6 – PLANNING **Goal:** Identify risks and opportunities, define objectives, and plan ISMS improvements. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 6.1.1 Actions to Address Risks and Opportunities | * Conduct a gap analysis and define security opportunities (e.g., zero-trust, CSPM tools). Include them in your ISMS improvement plan. | Risk Manager, CISO | * SWOT analysis * Improvement roadmap | COBIT APO12, NIST CSF ID.RA-1, ISO 31000 |
| 6.1.2 Information Security Risk Assessment | * Perform formal risk assessment. * Score risks by impact & likelihood. | Risk Lead, Product Security | * Risk register * Methodology doc * Jira tickets | NIST SP 800-30, PCI DSS 12.2, HIPAA 164.308(a)(1)(ii)(A) |
| 6.1.3 Information Security Risk Treatment | * Define mitigation actions for unacceptable risks. * Map selected controls to Annex A. | CISO, Engineering Manager | * Risk treatment plan * Control justification record | NIST SP 800-53 RA-3, ISO 27005, COBIT DSS01 |
| 6.2 Security Objectives and Planning | * Set measurable ISMS objectives (e.g., “100% critical patch SLA compliance within 15 days”) and define tracking metrics. | CISO, IT Ops Lead | * Metrics dashboard * OKRs * Project trackers | NIST CSF ID.GV-3, COBIT MEA01, HIPAA 164.308(a)(8) |
| 6.3 Planning of Changes | * Build a change management process to handle policy, tool, or scope changes without disrupting ISMS operations. | Change Advisory Board, Security PM | * Change log * Version control records * Policy update forms | NIST SP 800-128, COBIT BAI06, PCI DSS 6.4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CLAUSE 7 – SUPPORT **Goal:** Ensure your organization has the resources, skills, awareness, and documentation needed to operate and sustain the ISMS. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 7.1 Resources | * Identify and allocate financial, technical, and human resources to support security initiatives. | CISO, COO, Finance Lead | * Budget plans * Staff headcount charts * Vendor contracts | NIST SP 800-53 PM-3, COBIT APO07, NIST CSF ID.BE-4 |
| 7.2 Competence | * Define required skills (e.g., DevSecOps, AWS IAM). * Verify staff qualifications. * Deliver targeted training. | HR, Security Manager | * Training logs * Employee resumes and certifications (e.g., CISSP, AWS SAA) | NIST SP 800-53 AT-3, HIPAA 164.308(a)(5)(ii)(B), PCI DSS 12.6 |
| 7.3 Awareness | * Run security awareness campaigns (e.g., phishing simulations, onboarding modules). | Security Awareness Lead | * Quiz scores * Phishing test reports * LMS records | NIST SP 800-53 AT-2, CCPA §1798.100, COBIT DSS05 |
| 7.4 Communication | * Establish internal/external comms strategy (e.g., security newsletter, breach notification SOPs). | Comms Lead, DPO, CISO | * Communication plan * Email templates * Incident comms workflows | GDPR Art. 33, NIST CSF RS.CO-5, PCI DSS 12.10.1 |
| 7.5.1 Documented Information – General | * Define what policies, procedures, and logs are required for ISMS operation and control. | Documentation Owner, CISO | * Document register * ISMS index * Policy archive | COBIT MEA02, NIST SP 800-53 PL-2 |
| 7.5.2 Creating and Updating | * Establish version control, ownership, and review timelines for each document. | Policy Manager, ISMS Admin | * Version history * Change requests * Approval signatures | ISO 9001 Clause 7.5, PCI DSS 12.1.1 |
| 7.5.3 Control of Documented Information | * Restrict access to sensitive docs (e.g., risk assessments), back up securely, and audit views or changes. | IT Ops, GRC Team | * DMS logs * ACL records * Backups * Retention policies | NIST SP 800-53 CM-9, HIPAA 164.316(b)(1), COBIT APO03 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CLAUSE 8 – OPERATION **Goal:** Operate the ISMS by planning, executing, and monitoring security-related processes and risk treatments effectively. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 8.1 Operational Planning and Control | * Implement necessary controls for managing infrastructure, customer data, and third-party dependencies. * Ensure secure CI/CD pipelines, change management, and access control. | Engineering Manager, DevOps Lead | * Operational procedures * CI/CD pipeline security docs * SOC 2 mapping sheets | NIST SP 800-53 AC-1, CM-2, COBIT DSS01, PCI DSS 6.4 |
| 8.2 Information Security Risk Assessment | * Perform regular re-assessments of risks tied to products, environments, and new features or business changes. | Risk Analyst, Product Security | * Risk re-evaluation logs * Updates to the risk register * Change tracking | NIST SP 800-30, NIST CSF ID.RA-5, COBIT APO12 |
| 8.3 Information Security Risk Treatment | * Implement and monitor mitigation plans. (For example, integrate automated misconfiguration alerts in AWS or enforce secure defaults in code.) | Engineering Lead, AppSec | * Control implementation tracker * Vulnerability patch reports * Mitigation evidence | NIST SP 800-53 RA-7, HIPAA 164.308(a)(1)(ii)(B), PCI DSS 12.2.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CLAUSE 9 – PERFORMANCE EVALUATION **Goal:** Monitor and assess the performance of the ISMS to ensure controls are effective, risks are being managed, and continual improvement is driven by data. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 9.1 Monitoring, Measurement, Analysis and Evaluation | * Define KPIs (e.g., vulnerability remediation SLAs, DLP alert resolution). * Collect relevant metrics. * Evaluate ISMS effectiveness quarterly. | GRC Lead, CISO | * KPI dashboard * Metric reports * Trend analysis * SIEM dashboards | NIST CSF MEA-1, HIPAA 164.308(a)(8), COBIT MEA01 |
| 9.2 Internal Audit | * Plan and conduct annual ISMS audits using an audit program. * Identify nonconformities and track remediation (e.g., Jira tickets, Confluence logs). | Internal Auditor, CISO | * Audit plan and reports * NCR logs * Follow-up reports | NIST SP 800-53 CA-7, COBIT MEA03, PCI DSS 12.11 |
| 9.3 Management Review | * Conduct leadership reviews (at least annually) to assess ISMS status, including policy changes, incidents, audits, risk trends, and objectives. | CISO, Executive Team | * Review meeting minutes * Policy revision decisions | ISO 9001 Clause 9.3, COBIT EDM03, NIST CSF ID.GV-4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ANNEX A.5 — ORGANIZATIONAL CONTROLS **Goal:** Establish comprehensive organizational governance by defining policies, roles, risk management, asset inventory, supplier oversight, and response plans that support and sustain secure operations. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| A.5.1 – Policies for Information Security | * Develop a high-level Information Security Policy aligned to business objectives. * Have it approved by leadership and communicate it to staff. * Review it annually or after major changes. | CISO, Compliance Officer | * Information Security Policy * Version history * Leadership approval log * Intranet publication record | NIST CSF ID.GV-1, NIST SP 800-53 PL-1, HIPAA 164.308(a)(1), PCI DSS 12.1, COBIT APO01, GDPR Art. 24 |
| A.5.2 – Information Security Roles & Responsibilities | * Define key ISMS roles and duties with responsibilities mapped to job titles. * Create and publish a responsibility matrix (e.g., RACI) and integrate into onboarding. | HR, CISO | * RACI matrix * Org. chart with job descriptions * Onboarding checklist | NIST SP 800-53 AT-1, HIPAA 164.308(a)(2), PCI DSS 12.4, COBIT BAI09 |
| A.5.3 – Segregation of Duties | * Implement technical and procedural controls to divide sensitive responsibilities. * Enforce separation in production access, code deployments, financial approvals. | Engineering Manager, IAM Analyst | * Access control matrix * Audit logs * Privileged access reviews * DevOps role mapping | NIST SP 800-53 AC-5, PCI DSS 7.2.2, COBIT DSS06, CCPA §1798.100(d) |
| A.5.4 – Management Responsibilities | * Assign accountability for ISMS enforcement to business unit leaders. * Set expectations for reporting, incident escalation, and compliance. * Integrate with KPIs or OKRs. | Department Heads, CEO | * Departmental ISMS ownership docs * KPI/OKR dashboards * Leadership meeting records | NIST CSF ID.GV-1, COBIT APO01, ISO/IEC 27001 Clause 5.1 |
| A.5.5 – Contact with Authorities | * Identify relevant authorities (e.g., regulators, cybercrime units, data protection authorities). * Maintain up-to-date contact records and incident response procedures. | Compliance Officer, DPO | * Contact list * Incident response plan with legal liaison procedures | NIST SP 800-53 IR-6, HIPAA 164.308(a)(6), GDPR Art. 31, COBIT DSS02 |
| A.5.6 – Contact with Special Interest Groups | * Join industry groups, SaaS security forums, or ISACs. * Share and receive threat intel, regulatory changes, and security trends. | CISO, Threat Intel Lead | * Membership confirmations * Participation logs * Knowledge-sharing memos | NIST CSF ID.RA-2, ISO 27001 4.2, COBIT APO02 |
| A.5.7 – Threat Intelligence | * Gather and assess threat intelligence relevant to your stack (e.g., CVEs for cloud tech). * Integrate with your risk register and update controls accordingly. | Threat Intel Analyst, SOC Lead | * Threat intel feeds * Vendor alerts * Correlation rules in SIEM * Recorded monthly threat briefings | NIST SP 800-53 RA-5, NIST CSF DE.CM-6, PCI DSS 12.2.1 |
| A.5.8 – Information Security in Project Management | * Embed security reviews in project lifecycles — include threat modeling, data flow assessments, and architecture reviews for all product launches or internal tools. | Project Managers, AppSec Lead | * Secure SDLC checklist * Risk assessments in project files * Review signoffs | NIST SP 800-64, COBIT BAI03, HIPAA 164.308(a)(1)(ii)(D) |
| A.5.9 – Inventory of Information and Other Associated Assets | * Maintain an up-to-date inventory of assets: customer data types, cloud resources, devices, codebases. Include owners and classification. * Automate where possible using CMDB or cloud inventory tools. | IT Asset Manager, Security Engineer | * Asset register * CMDB exports * S3/GCP/Azure inventories * Ownership assignments | NIST SP 800-53 CM-8, PCI DSS 2.4, HIPAA 164.310(d)(1), COBIT BAI09 |
| A.5.10 – Acceptable Use of Information and Other Associated Assets | * Define acceptable use of laptops, admin consoles, cloud dashboards, and customer data. * Communicate via onboarding, policies, and reminders. | HR, IT Manager | * Acceptable Use Policy * Signed acknowledgment forms * Training records | NIST SP 800-53 AC-17, HIPAA 164.308(a)(3), PCI DSS 12.3, COBIT DSS01 |
| A.5.11 – Return of Assets | * Ensure recovery of laptops, tokens, access cards, credentials, and source code access at contract end or termination. * Automate offboarding. | HR, IT Support, Security Analyst | * Termination checklist * Offboarding logs * IAM revocation reports | NIST SP 800-53 PS-4, ISO/IEC 27002:2022 A.5.11, COBIT DSS04 |
| A.5.12 – Classification of Information | * Classify data (e.g., Public, Internal, Confidential, Restricted) and apply controls based on sensitivity. * Define examples within your environment: PII, config files, API secrets. | Data Governance Lead, Compliance Officer | * Data classification policy * Examples matrix * DLP policy * Automated labels | NIST SP 800-60, GDPR Art. 32, HIPAA 164.312(c), COBIT APO03 |
| A.5.13 – Labelling of Information | * Establish labeling standards for different data classifications (e.g., “Confidential”, “Internal Use Only”). * Apply via document templates, DLP tags, or metadata. | Data Governance Lead, IT Admin | * Labeling guide * Tagged documents/emails * DLP policy config | NIST SP 800-53 MP-3, GDPR Art. 32, COBIT DSS01 |
| A.5.14 – Transfer of Information | * Define and enforce secure methods for data transfers (e.g., SFTP, TLS 1.2+, encrypted email). * Prohibit unapproved tools (e.g., personal Dropbox, USBs). | IT Security Engineer, DPO | * Secure transfer policy * Email DLP rules * Cloud sharing restrictions | NIST SP 800-53 SC-12/SC-13, HIPAA 164.312(e), PCI DSS 4.1, COBIT DSS05 |
| A.5.15 – Access Control | * Define role-based access control (RBAC) policies for systems and platforms. Include provisioning, deprovisioning, and regular access reviews. | IAM Lead, Security Admin | * RBAC policy * Access logs * Quarterly review records * Onboarding/offboarding procedures | NIST SP 800-53 AC-2/AC-6, HIPAA 164.308(a)(4), PCI DSS 7.1, COBIT DSS06 |
| A.5.16 – Identity Management | * Implement centralized identity federation (e.g., SSO via Okta/Azure AD). * Manage identity lifecycle events with workflows and access approval gates. | IAM Administrator, IT Manager | * Identity policy * Workflow documentation * SSO config * Access request forms | NIST SP 800-63-3, NIST SP 800-53 IA-2, COBIT DSS05, CCPA §1798.100 |
| A.5.17 – Authentication Information | * Define password and authentication policies. * Enforce strong password controls and MFA for all privileged and customer-facing systems. * Avoid shared credentials. | Security Engineer, IAM Admin | * Password policy * MFA logs * SSO audit trails * Vault config | NIST SP 800-63B, NIST SP 800-53 IA-5, PCI DSS 8.3, HIPAA 164.312(d) |
| A.5.18 – Access Rights | * Ensure that access rights (create, read, update, delete) are aligned to job roles. * Review access regularly and revoke excess permissions promptly. | CISO, IAM Analyst | * Quarterly access review reports * User-role mapping matrix * Deprovisioning logs | NIST SP 800-53 AC-2(7), HIPAA 164.308(a)(4), PCI DSS 7.2.1, COBIT DSS01 |
| A.5.19 – Information Security in Supplier Relationships | * Evaluate suppliers for security controls. * Use due diligence checklists and security addenda in contracts. * Classify third parties by data access risk. | Procurement, Compliance Officer | * Supplier risk matrix * Due diligence forms * Vendor SOC 2/ISO 27001 certificates | NIST SP 800-53 SR-3/SR-5, ISO 27036, GDPR Art. 28, COBIT APO10 |
| A.5.20 – Addressing Information Security in Supplier Agreements | * Add security clauses to contracts, including data handling, incident reporting, audit rights, and termination requirements. | Legal Counsel, Vendor Manager | * Signed supplier agreements * Security clauses * DPA templates | NIST SP 800-53 SA-9, PCI DSS 12.8.2, HIPAA 164.308(b), CCPA §1798.140(f) |
| A.5.21 – Managing Information Security in the ICT Supply Chain | * Assess supplier risk for cloud services, infrastructure providers, and tools. * Track service types, access levels, and contract terms. * Monitor supply chain threats. | Security Manager, Procurement | * Supply chain inventory * Vendor risk assessments * Security ratings * SLA reviews | NIST SP 800-53 SR-2/SR-5, ISO 27036, COBIT APO10, PCI DSS 12.8.5 |
| A.5.22 – Monitoring, Review, and Change Management of Supplier Services | * Periodically review supplier performance and risk (e.g., data handling, SLA uptime, security posture). * Document changes and enforce reapproval. | Vendor Manager, Legal, Compliance | * Supplier audit logs * Performance scorecards * Contract amendment records | COBIT MEA03, NIST CSF ID.BE-5, HIPAA 164.308(b)(1) |
| A.5.23 – Information Security for Use of Cloud Services | * Define and document a cloud governance policy. * Require baseline controls for SaaS, PaaS, IaaS providers (e.g., encryption, logging, admin access limits). | Cloud Security Architect, DevOps | * CSPM reports * Cloud security checklist * Cloud policy * AWS/Azure/GCP baseline docs | NIST SP 800-144, ISO 27017, CIS Benchmarks, CCPA §1798.100(e) |
| A.5.24 – Information Security Incident Management Planning and Preparation | * Build an incident response plan covering cloud breaches, SaaS availability incidents, customer data exposure. Align with NIST/ISO frameworks. * Test at least annually. | Incident Response Lead, CISO | * Incident Response Plan * Tabletop exercise reports * Escalation matrix | NIST SP 800-61, PCI DSS 12.10, HIPAA 164.308(a)(6), COBIT DSS04 |
| A.5.25 – Assessment and Decision on Information Security Events | * Define criteria to identify events vs. incidents. * Implement alert triage workflows in the SOC or security team to assess severity and take action. | SOC Manager, Security Analyst | * Event classification matrix * SIEM alert response guide * Triage checklist | NIST SP 800-61, NIST SP 800-53 IR-4, COBIT DSS02, PCI DSS 10.6.1 |
| A.5.26 – Response to Information Security Incidents | * Respond to validated incidents using defined procedures. * Document steps taken, contain impact, and notify stakeholders as required (e.g., customer breach comms). | IR Team, CISO, DPO | * Incident tickets * Response timelines * Communication logs * Customer notice templates | NIST SP 800-61, HIPAA 164.308(a)(6), GDPR Art. 33, PCI DSS 12.10.5 |
| A.5.27 – Learning from Information Security Incidents | * Conduct post-incident reviews and root cause analysis (RCA). * Document lessons learned and update controls/policies. * Feed into continuous improvement process. | Risk Manager, CISO | * RCA reports * Incident retrospectives * Control updates * Process change logs | COBIT MEA02, NIST SP 800-53 IR-8, ISO 27001 Clause 10.1 |
| A.5.28 – Collection of Evidence | * Define procedures for preserving evidence integrity (e.g., log retention, forensic imaging). * Train staff on chain of custody principles. | IR Lead, Security Operations | * Evidence handling SOPs * Forensic image metadata * Chain-of-custody forms | NIST SP 800-86, PCI DSS 12.10.7, ISO 27037, COBIT DSS01 |
| A.5.29 – Information Security During Disruption | * Maintain security controls during business continuity or DR scenarios. * Include fallback processes for IAM, logging, and customer support in downtime. | BCP Manager, Security Architect | * BCP with security clauses * Backup authentication procedures * DR drills | NIST SP 800-34, ISO 22301, HIPAA 164.308(a)(7), COBIT DSS04 |
| A.5.30 – ICT Readiness for Business Continuity | * Evaluate readiness of IT systems to support continuity. * Ensure backups, redundant systems, and RTO/RPOs are defined and tested. | IT Manager, Infra Lead | * Backup test logs * Failover plans * RTO/RPO documentation * Uptime tracking | NIST SP 800-34 Rev.1, PCI DSS 12.10.6, COBIT DSS03 |
| A.5.31 – Legal, Statutory, Regulatory, and Contractual Requirements | * Identify and document applicable legal and regulatory requirements (e.g., GDPR, HIPAA, SOC 2). * Integrate them into ISMS and risk assessments. | Legal, Compliance Officer | * Compliance register * Data protection mapping * Audit prep logs | GDPR Art. 5/6, HIPAA 164.306, COBIT APO12, CCPA §1798.100 |
| A.5.32 – Intellectual Property Rights | * Protect IPR by managing software licenses, internal code repositories, and copyright/IP clauses in contracts. * Monitor open source usage. | Legal Counsel, Engineering Lead | * IP protection policy * License tracking logs * OSS audit tools | NIST SP 800-53 PL-8, ISO 27001 A.5.32, COBIT APO09 |
| A.5.33 – Protection of Records | * Maintain integrity and availability of SaaS audit logs, legal documents, and transaction records. * Define retention and disposal rules. | Records Manager, IT Admin | * Data retention policy * Archive logs * Record access tracking | NIST SP 800-53 AU-11, HIPAA 164.312(c)(1), PCI DSS 10.7 |
| A.5.34 – Privacy and Protection of PII | * Implement controls to ensure compliance with privacy laws (e.g., GDPR, CCPA). Include consent management, data minimization, and access logging. | DPO, Compliance Officer | * Privacy policy * Consent logs * DSAR tracker * Encryption reports | GDPR Art. 32, CCPA §1798.100, HIPAA 164.502, NIST SP 800-122 |
| A.5.35 – Independent Review of Information Security | * Schedule annual internal or external ISMS reviews. Include policy coverage, risk alignment, and control maturity. | Internal Auditor, CISO | * Audit schedule * Review reports * Remediation tracking | ISO 27001 Clause 9.2, NIST SP 800-53 CA-2, COBIT MEA03 |
| A.5.36 – Compliance with Policies and Standards | * Monitor staff compliance with internal ISMS policies. * Automate detection of violations and follow up with corrective actions. | GRC Analyst, Security Awareness Lead | * Audit findings * Awareness training completion rates * Policy violation logs | HIPAA 164.308(a)(1)(ii)(D), COBIT MEA02, PCI DSS 12.6.2 |
| A.5.37 – Documented Operating Procedures | * Maintain documented SOPs for key operations (e.g., deployment, incident response, backup). * Review and update regularly. | Operations Manager, DevOps Lead | * SOP repository * Version logs * Team playbooks * CI/CD runbooks | NIST SP 800-53 CP-2, ISO 27001 Clause 7.5, COBIT BAI01 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ANNEX A.6 — PEOPLE CONTROLS **Goal:** Establish comprehensive organizational governance by defining policies, roles, risk management, asset inventory, supplier oversight, and response plans that support and sustain secure operations. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| A.6.1 – Screening | * Perform pre-employment background checks, reference verification, and criminal history reviews aligned to role sensitivity (e.g., DevOps, DBAs). | HR, Legal | * Background check confirmations * Risk tiering by role * Offer letter templates | NIST SP 800-53 PS-3, HIPAA 164.308(a)(3)(ii)(B), COBIT BAI03 |
| A.6.2 – Terms and Conditions of Employment | * Include security obligations (confidentiality, IP protection, acceptable use) in offer letters and employment contracts. * Require acknowledgment during onboarding. | HR, Legal | * Signed agreements * HR onboarding checklist * Contract templates | GDPR Art. 28, HIPAA 164.308(a)(3), COBIT DSS01 |
| A.6.3 – Information Security Awareness, Education and Training | * Deliver recurring training on SaaS-relevant topics (e.g., phishing, MFA, insider threats, secure code). * Include this training during onboarding and at regular intervals. | Security Awareness Lead, HR | * LMS completion records * Training calendar * Phishing simulation reports | NIST SP 800-53 AT-2, PCI DSS 12.6, HIPAA 164.308(a)(5) |
| A.6.4 – Disciplinary Process | * Define consequences for non-compliance with InfoSec policies. * Ensure processes are consistent, fair, and enforceable. * Align processes with HR policies. | HR, Legal, Compliance | * Disciplinary policy * Violation case records * Incident escalations | COBIT MEA03, ISO 27002:2022 A.6.4, NIST SP 800-53 PS-8 |
| A.6.5 – Responsibilities After Termination or Change of Employment | * Ensure removal or adjustment of access rights upon role change or departure. * Reclaim company assets and update NDAs if needed. | HR, IT Support, IAM Admin | * Termination checklist * Exit interview logs * Deprovisioning evidence * Asset return forms | NIST SP 800-53 PS-4, HIPAA 164.308(a)(3)(ii)(C), COBIT DSS05 |
| A.6.6 – Confidentiality or Non-Disclosure Agreements | * Use NDAs to protect proprietary and customer information. Apply to employees, contractors, and third parties. * Renew or enforce post-employment if necessary. | Legal, HR | * NDA templates * Signed copies * Contract clauses * Renewal logs | GDPR Recital 39, HIPAA 164.502(b), NIST SP 800-53 PL-4 |
| A.6.7 – Remote Working | * Enforce secure practices for remote access: VPN, MFA, endpoint protection. * Provide clear policy on use of personal devices and data handling at home. | IT Security Lead, HR, Compliance | * Remote work policy * VPN logs * Device inventory * Home office risk questionnaire | NIST SP 800-114, HIPAA 164.308(a)(1), PCI DSS 12.3.8, COBIT DSS01 |
| A.6.8 – Information Security Event Reporting | * Train staff to report suspicious behavior, phishing, and policy violations. * Create an easy-to-use reporting channel (e.g., ticketing system, anonymous form). | Security Awareness Lead, SOC Lead | * Incident report form * LMS records * Slack/Helpdesk channels * Escalation procedures | NIST SP 800-53 IR-6, PCI DSS 12.10.5, HIPAA 164.308(a)(6)(ii), COBIT DSS02 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ANNEX A.7 — PHYSICAL CONTROLS **Goal:** Protect physical environments that store or access sensitive SaaS infrastructure (e.g., office workstations, colocation data centers, networking closets) from unauthorized access, damage, or disruption. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| A.7.1 – Physical Security Perimeter | * Define and enforce access boundaries (e.g., locked doors, card readers) around secure work areas, server rooms, and sensitive paper storage. | Facilities Manager, Security Admin | * Floor plans * Badge access logs * Surveillance footage * Visitor access controls | NIST SP 800-53 PE-2, HIPAA 164.310(a)(1), PCI DSS 9.1, COBIT DSS01 |
| A.7.2 – Physical Entry | * Implement access controls (e.g., ID badges, keypads, security guards). * Enforce entry approval for visitors and restrict off-hours access. | Office Manager, IT | * Entry control policy * Visitor logs * Access control system exports | NIST SP 800-53 PE-3, PCI DSS 9.3–9.4, HIPAA 164.310(a)(2), COBIT DSS01 |
| A.7.3 – Securing Offices, Rooms, and Facilities | * Protect areas where staff access production systems or sensitive information. * Lock unattended offices and enforce key/code management. | Facilities Lead, Security Admin | * Lock/key register * Badge system audit logs * Security walkthrough checklists | ISO 27001 A.7.3, NIST SP 800-53 PE-5, COBIT DSS01 |
| A.7.4 – Physical Security Monitoring | * Use video surveillance and alarm systems in key areas (e.g., IDF closets, colocation cages). * Monitor entry and investigate suspicious activity. | Security Team, Facilities | * Camera placement documentation * DVR logs * Alarm test results | NIST SP 800-53 PE-6, PCI DSS 9.1.1, COBIT DSS01 |
| A.7.5 – Protection Against Physical and Environmental Threats | * Ensure protection against fire, flooding, HVAC failure, power loss, and natural disasters. * Perform site risk assessments and monitor critical environment conditions. | Facilities Manager, IT | * Environmental risk assessment * Fire alarm system test logs * Temperature/humidity logs * Generator test results | NIST SP 800-53 PE-10/PE-13, HIPAA 164.310(b), PCI DSS 9.1.1, COBIT DSS04 |
| A.7.6 – Working in Secure Areas | * Restrict access and enforce strict behavior in secure areas. * Define rules for escorting visitors, prohibited devices (e.g., phones), and clean desk policies. | IT Security Lead, Office Manager | * Secure area policy * Posted signage * Visitor escort logs * Badge audits | NIST SP 800-53 PE-16, ISO/IEC 27002:2022 A.7.6, COBIT DSS01 |
| A.7.7 – Clear Desk and Clear Screen Policy | * Require users to lock screens and secure paper documents when unattended. Include in onboarding and perform periodic checks or walk-throughs. | HR, Security Awareness Lead | * Clear desk policy * Training records * Spot check logs * IT monitoring tool configs | NIST SP 800-53 AC-11, HIPAA 164.310(d), COBIT DSS05 |
| A.7.8 – Equipment Siting and Protection | * Locate equipment to minimize environmental risks and unauthorized access. * Avoid placing critical infrastructure near windows, vents, or public areas. | IT Manager, Facilities | * Rack placement diagrams * Access restriction photos * Equipment risk assessments | NIST SP 800-53 PE-18, PCI DSS 9.1.1, ISO 27001 A.7.8 |
| A.7.9 – Security of Assets Off-Premises | * Establish controls for securing laptops, mobile devices, and paper files taken off-site. * Enforce encryption, endpoint protection, and use of VPN when accessing customer or production data remotely. | IT Support, Remote Work Coordinator | * Off-prem policy * Device encryption logs * VPN usage reports * Mobile asset inventory | NIST SP 800-53 MP-7, HIPAA 164.310(d), PCI DSS 12.3.6, COBIT DSS01 |
| A.7.10 – Storage Media | * Define policies for managing storage media (e.g., USB drives, backup tapes, external HDDs). * Limit usage, encrypt sensitive media, and track inventory. | IT Admin, Security Engineer | * Media use policy * Encryption reports * Removable media logs * Asset tag register | NIST SP 800-88, HIPAA 164.310(d)(1), PCI DSS 9.8, COBIT DSS01 |
| A.7.11 – Supporting Utilities | * Ensure availability and resilience of utilities that support IT systems (e.g., power, HVAC, UPS). * Regularly test and maintain equipment. | Facilities Manager, IT Ops Lead | * Power backup test logs * HVAC maintenance reports * Uptime SLA records | NIST SP 800-53 PE-11/PE-12, PCI DSS 12.5.2, ISO 22301, COBIT DSS03 |
| A.7.13 – Equipment Maintenance | * Define maintenance schedules and service-level expectations for critical equipment (e.g., servers, firewalls, UPS). * Use trusted vendors and track service activities. | IT Ops Manager, Vendor Manager | * Maintenance logs * Vendor service records * SLA documentation * Downtime logs | NIST SP 800-53 MA-2, PCI DSS 9.1.1, COBIT DSS01 |
| A.7.14 – Secure Disposal or Reuse of Equipment | * Sanitize storage devices using approved data destruction methods before reuse, resale, or disposal. * Maintain disposal logs and certificates of destruction. | IT Support, Asset Manager | * Device sanitization checklist * Wipe logs * Destruction certificates * Disposal policy | NIST SP 800-88, HIPAA 164.310(d)(2), PCI DSS 9.8.2, COBIT DSS01 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ANNEX A.8 — TECHNOLOGICAL CONTROLS **Goal:** Protect SaaS platforms, infrastructure, and customer data using secure configurations, technical safeguards, monitoring systems, encryption, secure development, and robust identity and access controls. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| A.8.1 – User Endpoint Devices | * Enforce endpoint hardening (e.g., EDR, disk encryption, patching, screen lock). * Apply policies to corporate laptops and BYOD. * Monitor compliance via MDM. | IT Support, Security Engineer | * EDR logs * MDM dashboard * Encrypted disk reports * Device compliance checks | NIST SP 800-53 CM-7, HIPAA 164.310(d), PCI DSS 12.3.6, COBIT DSS01 |
| A.8.2 – Privileged Access Rights | * Limit and monitor the use of privileged accounts. * Enforce least privilege and separation of roles. * Require MFA and session logging for admin access. | IAM Lead, Infrastructure Manager | * Privileged access policy * Audit logs * User-role mapping * PAM system reports | NIST SP 800-53 AC-6(10), PCI DSS 7.2.2, HIPAA 164.308(a)(4), COBIT DSS06 |
| A.8.3 – Information Access Restriction | * Apply RBAC and attribute-based access to systems and production environments. * Restrict access based on business need and data classification. | Application Owner, Security Architect | * Access control policy * RBAC configs * IAM logs * Entitlement reviews | NIST SP 800-53 AC-2/AC-3, PCI DSS 7.1, HIPAA 164.308(a)(4), CCPA §1798.100 |
| A.8.4 – Access to Source Code | * Restrict access to repositories based on role. * Require code reviews, protect against source code leaks, and log all Git interactions. | DevOps Lead, AppSec Engineer | * Git permissions config, audit trails, SAST findings, merge review evidence | NIST SP 800-53 CM-5, ISO 27034, COBIT BAI03 |
| A.8.5 – Secure Authentication | * Enforce strong authentication (e.g., MFA, SSO, device-based trust). Avoid password reuse and shared credentials. * Apply phishing-resistant MFA for admin access. | IAM Engineer, Security Architect | * MFA policy * IdP configuration screenshots * Login attempt logs * Password rotation evidence | NIST SP 800-63B, HIPAA 164.312(d), PCI DSS 8.3, CCPA §1798.100 |
| A.8.6 – Capacity Management | * Monitor SaaS infrastructure capacity (e.g., compute, storage, bandwidth). * Define thresholds and autoscaling policies to avoid performance bottlenecks. | DevOps Lead, Infrastructure Manager | * Grafana/Datadog dashboards * Incident records * Performance tuning logs | NIST SP 800-53 CP-2, COBIT BAI09, ISO 27002 A.8.6 |
| A.8.7 – Protection Against Malware | * Deploy endpoint protection and email security filters. * Scan file uploads and block high-risk attachments. * Enable threat detection in cloud workloads. | SOC Lead, Security Engineer | * AV/Malware logs * Threat intelligence updates * Sandbox reports * EDR alerts | NIST SP 800-53 SI-3, HIPAA 164.308(a)(5), PCI DSS 5.1, COBIT DSS05 |
| A.8.8 – Management of Technical Vulnerabilities | * Continuously scan for vulnerabilities in systems, containers, and code. * Define SLAs for patching based on CVSS score. * Track exceptions and remediation efforts. | AppSec Lead, DevOps Manager | * Vulnerability scan reports * Jira remediation tickets * Patch cycle logs | NIST SP 800-40, NIST SP 800-53 RA-5, PCI DSS 6.2, HIPAA 164.308(a)(1) |
| A.8.9 – Configuration Management | * Enforce secure baseline configurations across servers, containers, cloud services, and apps. Automate via IaC. * Version and document all changes. | DevOps Lead, Infrastructure Security | * CIS benchmark results * Terraform/CloudFormation files * Config hardening checklists | NIST SP 800-53 CM-2/CM-6, PCI DSS 2.2, COBIT BAI10 |
| A.8.10 – Information Deletion | * Define data deletion procedures (manual and automated). * Wipe tenant data and logs per customer lifecycle or regulatory requirements. | Data Governance Lead, Infra Admin | * Deletion logs * Retention policies * Secure wipe confirmation (S3, RDS, etc.) | NIST SP 800-88, GDPR Art. 17, HIPAA 164.310(d)(2), CCPA §1798.105 |
| A.8.11 – Data Masking | * Apply masking or tokenization for lower environments (e.g., dev/test) or analytics use. * Prevent exposure of live customer PII to developers. | Data Engineering Lead, AppSec | * Masking policy * Tokenization platform logs * Anonymized dataset samples | NIST SP 800-53 SC-12, ISO 27002 A.8.11, HIPAA 164.312(a)(2)(iv) |
| A.8.12 – Data Leakage Prevention | * Deploy DLP controls on endpoints, email, and cloud storage (e.g., GDrive, S3). * Monitor for unauthorized file transfers or exposure of sensitive data. | SOC Analyst, Cloud Security Engineer | * DLP rules configuration * Alerts/reports * Outbound email monitoring evidence | NIST SP 800-53 SI-4, PCI DSS 11.4, CCPA §1798.150(c), COBIT DSS05 |
| A.8.13 – Information Backup | * Implement backup procedures for production databases, configs, and logs. * Automate cloud snapshots. * Define RPO/RTO and test restoration regularly. | DevOps Lead, IT Manager | * Backup policy, S3 lifecycle configs, backup logs, restore test results | NIST SP 800-53 CP-9, HIPAA 164.308(a)(7)(ii)(A), PCI DSS 12.5.1, COBIT DSS04 |
| A.8.14 – Redundancy of Information Processing Facilities | * Build redundancy for critical infrastructure (e.g., load balancers, databases, cloud zones). * Use autoscaling, failover systems, and DR regions. | Infrastructure Architect, Cloud Engineer | * HA architecture diagrams * Redundancy test results * Failover documentation | NIST SP 800-53 CP-10, ISO 22301, PCI DSS 12.1.2, COBIT DSS03 |
| A.8.15 – Logging | * Enable audit logging for cloud services, apps, endpoints, and platforms. * Log privileged commands, auth events, and data access. * Secure logs from tampering. | Security Engineer, DevOps | * Log configuration files * CloudTrail/Audit Logs * Tamper-proof storage setup | NIST SP 800-92, NIST SP 800-53 AU-2, PCI DSS 10.2, HIPAA 164.312(b) |
| A.8.16 – Monitoring Activities | * Monitor systems for anomalies, alerts, and security events using SIEM, CSPM, or custom tooling. * Define thresholds and escalation playbooks. | SOC Lead, Security Analyst | * SIEM alert dashboard * SOC playbooks * Alert triage records * MDR provider logs | NIST SP 800-53 AU-6, PCI DSS 10.6, HIPAA 164.308(a)(1)(ii)(D), COBIT DSS05 |
| A.8.17 – Clock Synchronization | * Synchronize system clocks across all critical infrastructure (e.g., cloud, databases, endpoints) using NTP. * Validate logs have accurate timestamps. | DevOps Lead, IT Admin | * NTP config files * System time audit logs * Clock sync reports | NIST SP 800-53 AU-8, PCI DSS 10.4, COBIT DSS01 |
| A.8.18 – Use of Privileged Utility Programs | * Restrict and monitor use of tools that bypass security mechanisms (e.g., debugging tools, password dumpers). * Audit their execution and enforce approval. | IT Security Admin, AppSec | * List of restricted tools * Shell history logs * PAM audit trails | NIST SP 800-53 AC-6(9), PCI DSS 10.2.2, COBIT DSS06 |
| A.8.19 – Installation of Software | * Control who can install software on endpoints and servers. Use whitelisting, signed packages, and centralized installation via MDM or DevOps pipelines. | IT Admin, DevOps | * Software approval logs * MDM restrictions * Package audit trails | NIST SP 800-53 CM-11, PCI DSS 2.2.1, COBIT BAI09 |
| A.8.20 – Networks Security | * Segment internal networks, use firewalls/WAFs, and monitor traffic for anomalies. * Secure APIs and ingress/egress points from public cloud. | Network Engineer, Cloud Security Architect | * Network topology * Firewall rules * IDS logs * Traffic analysis reports | NIST SP 800-53 SC-7, PCI DSS 1.2, HIPAA 164.312(c)(1), COBIT DSS05 |
| A.8.21 – Security of Network Services | * Ensure all third-party or internal network services (e.g., DNS, VPN, CDN) are configured securely. * Use encryption, access controls, and monitor SLAs. | Network Security Engineer, Vendor Manager | * Secure configuration docs * DNSSEC configs * VPN policies * Service contracts | NIST SP 800-53 SC-12, PCI DSS 1.2.1, COBIT DSS01 |
| A.8.22 – Segregation in Networks | * Enforce network segmentation between environments (e.g., prod vs. dev/test, admin vs. user) using subnets, VLANs, or cloud security groups. | Cloud Infrastructure Engineer, Security Architect | * Segmentation diagrams * VPC security group configs * Firewall rules | NIST SP 800-53 SC-7(1), PCI DSS 1.2.3, HIPAA 164.312(c)(1), COBIT DSS05 |
| A.8.23 – Web Filtering | * Apply URL and domain filtering on corporate devices and browsers to block malicious or non-business use. Monitor for high-risk destinations. | IT Admin, Security Operations | * Web filtering policy * DNS filter logs * Endpoint enforcement configurations | NIST SP 800-53 SC-18, PCI DSS 1.3.5, COBIT DSS05 |
| A.8.24 – Use of Cryptography | * Define a cryptography policy. Use strong encryption standards (e.g., AES-256, TLS 1.2+), manage keys securely, and retire weak algorithms. | Security Engineer, DevOps Lead | * Crypto inventory * KMS config * TLS scan results * Encryption policy | NIST SP 800-57, PCI DSS 3.5, HIPAA 164.312(a)(2)(iv), COBIT DSS05 |
| A.8.25 – Secure Development Life Cycle | * Define and enforce a Secure SDLC program that embeds security into requirements, design, coding, and deployment phases. * Use OWASP SAMM/ASVS. | AppSec Lead, Engineering Manager | * SDLC policy * Process docs * Secure design templates * Sprint tickets | NIST SP 800-53 SA-3, PCI DSS 6.3, COBIT BAI03 |
| A.8.26 – Application Security Requirements | * Document and review security requirements for all new features and services. Include authN/Z, data protection, and audit logging. | Product Owner, Security Architect | * Security requirement templates * Backlog tickets * Design review notes | ISO 27034, NIST SP 800-53 SA-17, GDPR Art. 25, COBIT BAI02 |
| A.8.27 – Secure System Architecture and Engineering Principles | * Apply secure-by-design principles in cloud infrastructure and architecture (e.g., least privilege, isolation, fail-secure). * Review changes via architecture boards. | Security Architect, Cloud Engineer | * Architecture review docs * Threat modeling outputs * Reference architecture diagrams | NIST SP 800-160, NIST SP 800-53 SA-8, COBIT BAI02 |
| A.8.28 – Secure Coding | * Enforce secure coding practices (e.g., input validation, error handling, no hardcoded secrets). * Provide developer training and code review standards. | Engineering Leads, AppSec | * Secure coding policy * Code review checklists * SAST results * Training records | OWASP Top 10, NIST SP 800-53 SA-11, PCI DSS 6.5, COBIT BAI03 |
| A.8.29 – Security Testing in Development and Acceptance | * Conduct SAST, DAST, dependency scanning, and manual reviews before releasing code. * Require testing as part of the CI/CD pipeline. | AppSec Engineer, QA Lead | * Security test reports * CI/CD logs * Jira stories with security sign-offs | NIST SP 800-53 SA-11, PCI DSS 6.3.2, COBIT BAI07 |
| A.8.30 – Outsourced Development | * Enforce security requirements and secure coding standards for third-party developers. * Include IP protection, review rights, and code scanning in contracts. | Engineering Manager, Legal | * Vendor contracts * Code access logs * External SAST reports * NDA documents | NIST SP 800-53 SA-9, HIPAA 164.308(b), COBIT BAI03 |
| A.8.31 – Separation of Development, Test and Production Environments | * Prevent mixing of dev, staging, and prod environments. * Block data copying from prod to test. * Enforce IAM boundaries and separate VPCs. | DevOps Engineer, Cloud Security Lead | * Network segmentation diagrams * IAM policies * Data redaction tools | NIST SP 800-53 CM-4, PCI DSS 6.4.1, COBIT DSS01 |
| A.8.32 – Change Management | * Require approval and testing for code and config changes. * Maintain audit trails and enforce rollback capabilities in CI/CD workflows. | Change Manager, DevOps Lead | * Change control logs * Pull Request reviews * CAB approvals * Rollback test results | NIST SP 800-128, PCI DSS 6.4.5, COBIT BAI06 |
| A.8.33 – Test Information | * Mask or anonymize sensitive data used in test environments. * Log access and prevent PII from being used in QA or development. | QA Lead, Data Governance | * Masked test datasets * Data handling policy * Test environment audit logs | NIST SP 800-53 SC-12, GDPR Art. 32, HIPAA 164.312(a)(2)(iv) |
| A.8.34 – Protection of Information Systems During Audit and Testing | * Prevent audit and testing activities from affecting production uptime or data confidentiality. * Use isolated environments and restrict access. | Security Engineer, Audit Coordinator | * Testing guidelines * Pre-audit impact assessment * Access control logs | NIST SP 800-53 AU-12, COBIT MEA02, ISO 27002 A.8.34 |

## FRAMEWORK REFERENCE SUMMARIES:

* **NIST CSF (Cybersecurity Framework)**

Developed by NIST, the CSF provides a risk-based, high-level framework for managing cybersecurity using five core functions: Identify, Protect, Detect, Respond, and Recover. It is widely adopted in both public and private sectors.

* **NIST SP 800 Series (Special Publications)**

A set of detailed technical standards and guidelines published by NIST, including foundational documents like SP 800-53 (controls catalog), SP 800-30 (risk assessment), and SP 800-37 (RMF). These are used by federal agencies and adopted widely by private organizations for building secure, compliant systems.

* **ISO/IEC 27001**

An international standard that specifies requirements for an Information Security Management System (ISMS). It provides a systematic approach to managing sensitive information through risk management, policies, procedures, and controls, and is often used to obtain certification.

* **HIPAA (Health Insurance Portability and Accountability Act)**

A U.S. regulation that sets standards for protecting sensitive health information (ePHI). HIPAA includes privacy, security, and breach notification rules applicable to healthcare providers, insurers, and their business associates.

* **PCI DSS (Payment Card Industry Data Security Standard)**

A security standard developed by major credit card companies that mandates technical and operational requirements for protecting cardholder data. Applicable to all entities that store, process, or transmit credit card data.

* **GDPR (General Data Protection Regulation)**

An EU regulation that governs the collection, use, and protection of personal data of individuals within the EU. It mandates consent, transparency, data rights, and security measures, and applies to any organization processing EU resident data.

* **COBIT (Control Objectives for Information and Related Technologies)**

An IT governance framework developed by ISACA that provides principles, practices, and tools for aligning IT management with business objectives, focusing on risk, compliance, performance, and control.

* **CCPA (California Consumer Privacy Act)**

A California law that gives consumers rights over their personal information, including access, deletion, and the ability to opt out of its sale. It applies to for-profit businesses meeting certain thresholds and requires transparency, data protection, and contractual controls with third parties.