**SOC 2 READINESS CHECKLIST:**

This document provides a step-by-step guide to help B2B SaaS companies prepare for a successful SOC 2 Type II audit. It outlines specific control actions, assigns responsibility, and maps each step to leading compliance frameworks including: COSO, 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 AICPA 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**

[CC1.0 - CONTROL ENVIRONMENT 2](#_Toc197096793)

[CC2.0 - COMMUNICATION AND INFORMATION 3](#_Toc197096794)

[CC3.0 – RISK ASSESSMENT 4](#_Toc197096795)

[CC4.0 – MONITORING ACTIVITIES 5](#_Toc197096796)

[CC5.0 – CONTROL ACTIVITIES 6](#_Toc197096797)

[CC6.0 – LOGICAL AND PHYSICAL ACCESS CONTROLS 7](#_Toc197096798)

[CC7.0 – SYSTEM OPERATIONS 9](#_Toc197096799)

[CC8.0 – CHANGE MANAGEMENT 10](#_Toc197096800)

[CC9.0 – RISK MITIGATION 11](#_Toc197096801)

[A1.0 – AVAILABILITY (OPTIONAL) 12](#_Toc197096802)

[C1.0 – CONFIDENTIALITY (OPTIONAL) 13](#_Toc197096803)

[PI1.0 – PROCESSING INTEGRITY (OPTIONAL) 15](#_Toc197096804)

[P1.0–P9.0 – PRIVACY (OPTIONAL) 16](#_Toc197096805)

[FRAMEWORK REFERENCE SUMMARIES: 19](#_Toc197096806)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC1.0 - CONTROL ENVIRONMENT **Goal:** Establish that leadership promotes a culture of integrity, accountability, and competence by defining roles, enforcing ethical standards, overseeing internal controls, and ensuring that employees understand and fulfill their control responsibilities. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **CORRESPONDING EVIDENCE** | **MAPPED FRAMEWORKS** |
| 1.1 **Goal:** Prove leadership enforces a culture of ethics and accountability. | * Define, approve, and publish Code of Conduct * Document ethical expectations | CEO, HR, Security Lead | * Signed Code of Conduct * Ethics training records * “Tone-at-the-top” CEO memo * Disciplinary policy and enforcement records | COSO Principle 1, NIST CSF ID.GV-1, NIST SP 800-53 PM-1, ISO A.5.1.1, HIPAA 164.308(a)(1)(i), PCI DSS 12.1, GDPR Recital 24, COBIT APO01, CCPA 1798.100(b) |
| 1.2 **Goal:** Demonstrate that senior leadership reviews and oversees risk, security posture, and compliance | * Assign board or executive oversight for security and risk * Review governance roles | CEO, Board, Security Committee | * Board meeting minutes discussing security * Audit committee charters * Org chart with board responsibilities * Security program updates * Risk or compliance reports presented to the board | COSO Principle 2, NIST CSF ID.GV-2, NIST SP 800-53 CA-6, ISO A.5.3.1, HIPAA 164.308(a)(2), PCI DSS 12.5, GDPR Art. 5(2), COBIT EDM01, CCPA 1798.135(a)(2) |
| 1.3 **Goal:** Confirm that roles and reporting structures are clearly defined and align with security and control responsibilities. | * Define reporting lines and control responsibilities * Establish org chart and role clarity | COO, HR, GRC Lead | * Org chart showing security leadership and lines of reporting * Job descriptions including control responsibilities * RACI matrix (Responsible, Accountable, Consulted, Informed) * Board-approved documentation defining executive and operational roles | COSO Principle 3, NIST SP 800-53 PM-3, ISO A.5.3.2, HIPAA 164.308(a)(3) |
| 1.4 **Goal:** Ensure personnel responsible for internal controls are appropriately skilled, trained, and supported. | * Attract and train competent staff * Define hiring requirements and onboarding processes | HR, GRC Lead, Department Managers | * New hire training logs * Security awareness LMS exports * Onboarding checklist * HR policy * Job postings with role-based security requirements | COSO Principle 4, NIST SP 800-53 AT-2, ISO A.7.2.2, HIPAA 164.308(a)(5), PCI DSS 12.6, GDPR Art. 39, COBIT BAI08.01 |
| 1.5 **Goal:** Demonstrate that employees and managers are aware of and responsible for executing their assigned control-related duties. | * Enforce accountability through reviews and disciplinary action * Align incentives to control compliance | HR, Department Managers, GRC Lead | * Performance review criteria referencing security objectives * Security responsibilities included in job descriptions * Signed Acceptable Use Policies (AUPs) * Policy enforcement procedures, policy violation records | COSO Principle 5, NIST SP 800-53 PL-4, ISO A.6.1.1, HIPAA 164.308(a)(1)(ii)(C) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC2.0 - COMMUNICATION AND INFORMATION **Goal:** Ensure that critical security and control information is clearly communicated across the organization and to external parties, enabling personnel and third parties to understand, perform, and support their internal control responsibilities. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 2.1 **Goal:** Verify that all personnel are informed of their roles, security policies, and operational expectations. | * Communicate relevant security and policy information internally (e.g., control awareness, updates) | GRC Lead, HR, Department Managers | * Internal security awareness communications (email, Slack, newsletters) * Training materials shared through LMS or intranet * Onboarding materials and internal documentation (Notion, Confluence) * Communication logs related to policy updates | COSO Principle 13, NIST CSF ID.GV-2, NIST SP 800-53 AT-3, IR-4, ISO A.7.2.2, HIPAA 164.308(a)(5)(i), PCI DSS 12.6.1, GDPR Art. 39(1)(b), COBIT BAI05.05, CCPA 1798.130(a)(6) |
| 2.2 **Goal:** Confirm that employees are clearly informed about their control responsibilities and the actions required to fulfill them. | * Define and communicate control responsibilities to relevant personnel | GRC Manager, HR, Functional Leads | * Control responsibility matrix (e.g., RACI chart) * Signed job descriptions with control roles * Internal wikis or playbooks assigning security tasks * Meeting notes or emails assigning specific control-related duties | COSO Principle 2, NIST CSF ID.GV-2, NIST SP 800-53 CA-6, ISO A.5.3.1, HIPAA 164.308(a)(2), PCI DSS 12.5, GDPR Art. 5(2), COBIT EDM01, CCPA 1798.135(a)(2) |
| 2.3 **Goal:** Confirm the organization shares relevant control requirements, expectations, and incident-related communications with vendors, partners, and clients. | * Communicate security/privacy expectations and contractual obligations to external parties (e.g., vendors, customers) | COO, HR | * Vendor security agreement or data processing addendum (DPA) * Client-facing security FAQ or documentation portal * Incident communication templates for customers and vendors * Vendor NDAs or third-party agreements referencing security obligations * Shared control responsibility matrix | COSO Principle 3, NIST SP 800-53 PM-3, ISO A.5.3.2, HIPAA 164.308(a)(3) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC3.0 – RISK ASSESSMENT **Goal:** Establish that the organization defines clear objectives and maintains a risk assessment process that identifies, evaluates, and tracks security, compliance, fraud, and change-related risks to ensure timely mitigation and control alignment. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 3.1 **Goal:** Confirm the company has clearly defined business and security objectives to evaluate risk against. | * Conduct a formal risk assessment identifying threats, vulnerabilities, and impact | GRC Lead, Security Team | * Documented strategic objectives * Risk assessment report with mapped objectives * Department-level goal documents * Information security policy referencing security objectives | COSO Principle 6, NIST CSF ID.RA-1, NIST SP 800-30, RA-1, ISO/IEC 27001 A.6.1.1, HIPAA 164.308(a)(1)(ii)(A), PCI DSS 12.2, GDPR Art. 24(1), COBIT APO12.01, CCPA 1798.100(b) |
| 3.2 **Goal:** Demonstrate that security, compliance, and operational risks are actively identified and tracked. | * Identify and prioritize risks to organizational objectives, including third-party/vendor risk | GRC, Engineering, Legal | * Risk register with risk categories and likelihood/impact * Threat modeling reports * Meeting minutes from risk workshops * Vendor risk evaluations and SOC 2 reports | COSO Principle 7, NIST CSF ID.RA-2, NIST SP 800-53 RA-2, RA-3, ISO A.6.1.2, PCI DSS 12.2, GDPR Art. 32, COBIT APO12.02 |
| 3.3 **Goal:** Ensure the risk assessment process includes evaluation of internal and external fraud risks. | * Include fraud and abuse scenarios in risk assessment | GRC, Legal, HR | * Risk register entries for fraud (e.g., insider threats, phishing) * Fraud prevention or detection policy * Audit logs with anomaly detection enabled * Whistleblower or ethics reporting procedures | COSO Principle 8, NIST CSF ID.RA-3, NIST SP 800-53 RA-3, AU-6(10), ISO A.6.1.3, HIPAA 164.312(c)(1), PCI DSS 10.2, GDPR Recital 75, COBIT APO12.03 |
| 3.4 **Goal:** Demonstrate that structural, environmental, or technological changes are assessed for their impact on security and control processes. | * Reassess risks due to internal/external change (e.g., infra migration, new vendors) | GRC, CTO, Compliance Lead | * Change impact assessment * Updated risk register * Documentation of system migrations or vendor transitions * Security review of architectural changes * Executive approvals or steering committee meeting notes | COSO Principle 9, NIST CSF ID.RA-4, NIST SP 800-53 CA-7, SA-5, ISO A.12.1.2, HIPAA 164.308(a)(8), PCI DSS 6.4.6, GDPR Art. 35, COBIT BAI06.05 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC4.0 – MONITORING ACTIVITIES **Goal:** Ensure the organization regularly evaluates the effectiveness of its internal controls through ongoing or periodic reviews and promptly remediates identified deficiencies with documented follow-up and accountability. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 4.1 **Goal:** Demonstrate that the company is actively reviewing its controls either continuously or through periodic assessments. | * Perform periodic or continuous reviews of system controls and policies | GRC Lead, Internal Audit, Control Owners | * Internal audit or compliance monitoring reports * SIEM dashboards with alert summaries * Ticket-based control checklists (e.g., quarterly access review tasks) | COSO Principle 16, NIST CSF DE.CM-7, NIST SP 800-53 CA-7, AU-6, ISO A.18.2.2, HIPAA 164.308(a)(8), PCI DSS 11.5, GDPR Art. 32(1)(d), COBIT MEA01.01 |
| 4.2 **Goal:** Confirm that internal control deficiencies are documented, escalated, and remediated with traceability. | * Track, report, and remediate control deficiencies * Document actions taken | GRC, Functional Owners, Management | * Internal audit reports or compliance findings * Jira or ServiceNow tickets tracking remediation tasks * Meeting minutes where issues and fixes were discussed * Updated risk register with control deficiency notes | COSO Principle 17, NIST CSF RS.CO-3, NIST SP 800-53 IR-6, CA-5, ISO A.16.1.3, HIPAA 164.308(a)(6)(ii), PCI DSS 12.10.5, GDPR Art. 33(5), COBIT MEA02.02 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC5.0 – CONTROL ACTIVITIES **Goal:** Ensure that the organization implements risk-aligned control activities, including foundational IT controls and documented policies and procedures, to consistently enforce security and operational safeguards across systems and teams. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 5.1 **Goal:** Verify that controls are implemented to mitigate the risks identified in the organization's risk assessment. | * Identify and implement control activities to mitigate risks from risk register | GRC Lead, Engineering, Control Owners | * Control matrix mapping risks to specific controls * Risk treatment plans * Policy references and associated control procedures * Approval of implemented controls by leadership or security team | COSO Principle 10, NIST CSF PR.IP-1, NIST SP 800-53 AC-1, CM-2, CM-3, ISO A.6.1.3, A.8.1.1, HIPAA 164.308(a)(1)(ii)(B), PCI DSS 6.1, GDPR Art. 24(1), COBIT DSS01.03, CCPA 1798.100(a)(1) |
| 5.2 **Goal:** Ensure that foundational IT controls (e.g., access management, change control, backup) are implemented consistently across systems. | * Establish and operate general IT controls (e.g., access, backups, change) | DevOps, IT Lead, Security | * Change management logs and approvals * Configuration management policies * Access control audit trails * Data backup configurations and logs | COSO Principle 11, NIST CSF PR.IP-3, NIST SP 800-53 CM-6, AC-3, CM-9, ISO A.12.1.2, A.14.2.2, HIPAA 164.308(a)(1)(ii)(C), PCI DSS 6.4, GDPR Art. 32(1), COBIT DSS05.03, CCPA 1798.100(d) |
| 5.3 **Goal:** Confirm that formal policies and procedures are documented, communicated, and implemented across relevant departments. | * Deploy and communicate policies and procedures to control owners and staff | GRC Lead, HR, Legal | * Published information security policies (PDFs or Confluence pages) * Procedure documents with step-by-step guidance * Policy acknowledgment logs from employees * Change logs showing version history and reviews | COSO Principle 12, NIST CSF PR.IP-4, NIST SP 800-53 PL-2, IR-1, MP-5, ISO A.5.1.2, HIPAA 164.308(a)(1)(ii)(D), PCI DSS 12.3–12.6, GDPR Art. 24(2), COBIT APO13.01, CCPA 1798.135(a)(2) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC6.0 – LOGICAL AND PHYSICAL ACCESS CONTROLS **Goal:** Ensure that logical and physical access to systems, data, and infrastructure is granted only to authorized individuals based on role and need; that access is monitored, revoked promptly when no longer required, and that removable media and sensitive assets are securely managed, logged, and disposed of in accordance with documented policies. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 6.1 **Goal:** Demonstrate that only authorized users can access protected systems and data, and that controls prevent unauthorized access. | * Implement role-based access control (RBAC) tied to least privilege | DevOps, Security Lead | * Role-based access matrix * Access request forms or Jira tickets with manager approval * Screenshot of MFA enabled across critical systems (e.g., AWS, GitHub) * Onboarding checklist with access provisioning steps * IAM policies or SSO group assignments (Okta, Azure AD) | COSO Principle 10, NIST CSF PR.AC-1, NIST SP 800-53 AC-2, AC-5, ISO A.9.2.1, HIPAA 164.308(a)(4)(ii)(B), PCI DSS 7.1.1, GDPR Art. 32(1)(b), COBIT DSS05.04, CCPA 1798.100(a)(1) |
| 6.2 **Goal:** Ensure user access is provisioned securely through a request-approval process and tied to defined roles. | * Provision logical access only after proper approval and based on job role | IT Admin, DevOps, HR | * Onboarding tickets or forms showing approval flow * User access provisioning checklists * Screenshots of SSO group assignment (Okta, Azure AD) * User access logs showing provisioning timestamps * Policy language defining access approval and documentation | COSO Principle 10, NIST CSF PR.AC-4, NIST SP 800-53 AC-6, AC-3, ISO A.9.1.2, HIPAA 164.312(a)(1), PCI DSS 7.1.2, GDPR Art. 25, COBIT APO07.06, CCPA 1798.130(a)(3)(B) |
| 6.3 **Goal:** Ensure access revocation is prompt, documented, and risk aware. | * Revoke access promptly upon termination or role change | HR, IT Admin | * Offboarding checklist with timestamps and de-provisioning confirmation * IAM logs showing deactivated users * Screenshots of group membership updates in Okta or Azure AD * Policy/procedure detailing access modification and removal timelines | COSO Principle 10, NIST CSF PR.AC-6, NIST SP 800-53 AC-2(3), ISO A.9.2.6, HIPAA 164.308(a)(3)(ii)(C), PCI DSS 8.1.4, GDPR Art. 25, COBIT DSS05.04, CCPA 1798.105(c) |
| 6.4 **Goal:** Demonstrate that physical access is controlled, monitored, and limited to those with a business need. | * Restrict physical access to facilities and devices | Ops Manager, Security Officer | * Physical access policy * Badge access logs with entry/exit records * List of employees with authorized access * Visitor sign-in logs and escort policy * Facility security camera logs or door sensor reports | COSO Principle 10, NIST CSF PR.AC-2, NIST SP 800-53 PE-2 to PE-6, ISO A.11.1.1, HIPAA 164.310(a)(1), PCI DSS 9.1–9.4, GDPR Art. 32(1), COBIT DSS01.04, CCPA 1798.100(d) |
| 6.5 **Goal:** Ensure sensitive physical assets are inventoried, monitored, and safeguarded with physical controls and protective procedures. | * Protect physical devices from loss or misuse | IT Lead, Security Team | * Asset inventory with tracking numbers and assigned owners * Laptop encryption and screen lock configurations * Device loss/theft reporting log * Physical lock or cable documentation for servers/equipment * MDM (Mobile Device Management) system screenshots | COSO Principle 10, NIST CSF PR.AC-5, NIST SP 800-53 PE-20, ISO A.11.2.6, HIPAA 164.310(d)(1), PCI DSS 9.9, GDPR Art. 32, COBIT DSS01.05, CCPA 1798.150(a)(1) |
| 6.6 **Goal:** Ensure removable media usage is controlled through policy, technical restrictions, and monitoring | * Restrict and monitor use of removable media | IT Admin, Security Lead | * Removable media policy (disable unless justified) * Endpoint protection software configuration screenshots * Logs showing use or attempted use of USB devices * List of approved encrypted drives * Documentation of media transport or handling | COSO Principle 10, NIST CSF PR.DS-3, NIST SP 800-53 MP-5, MP-7, ISO A.8.3.1–8.3.3, HIPAA 164.310(d)(1), PCI DSS 9.8.1, GDPR Art. 32, COBIT DSS05.07, CCPA 1798.150(a)(1) |
| 6.7 **Goal:** Confirm media disposal follows documented procedures that render data unrecoverable. | * Securely dispose of sensitive data and media | IT Lead, GRC | * Certificate of destruction from a third-party vendor * Media sanitization logs (e.g., DBAN, BitLocker) * Asset decommissioning checklist with approval * Disposal policy outlining acceptable methods (shredding, wiping, destruction) | COSO Principle 10, NIST CSF PR.IP-6, NIST SP 800-53 MP-6, ISO A.11.2.7, HIPAA 164.310(d)(2), PCI DSS 9.8.2, GDPR Art. 17, COBIT DSS05.08, CCPA 1798.105(c) |
| 6.8 **Goal:** Confirm that access and usage of systems are logged, reviewed, and retained to detect anomalies or violations. | * Monitor system and user access activity | Security Team, DevOps | * SIEM dashboards or security alert logs * Cloud provider audit logs (e.g., AWS CloudTrail, GCP, Okta) * Evidence of log reviews (Jira task or sign-off) * Policy requiring log retention and review | COSO Principle 10, NIST CSF DE.CM-3, DE.CM-7, NIST SP 800-53 AU-6, ISO A.12.4.1, HIPAA 164.308(a)(1)(ii)(D), PCI DSS 10.2, 10.6, GDPR Art. 32(1)(d), COBIT DSS05.02, CCPA 1798.150(a)(1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC7.0 – SYSTEM OPERATIONS **Goal:** Ensure the organization actively monitors system operations, detects and responds to security incidents, and maintains a documented vulnerability management process to identify, prioritize, and remediate threats to the environment. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 7.1 **Goal:** Confirm system-level monitoring is active and alerts are generated, reviewed, and acted upon. | * Enable infrastructure and application monitoring to detect system anomalies | DevOps, Security Team | * Alerting dashboards (e.g., Datadog, Splunk, Sentinel) * Logs showing detection of unusual activity * Documentation of incident triage * System health check reports with anomaly flags | COSO Principle 16, NIST CSF DE.CM-1, NIST SP 800-53 SI-4, AU-6, ISO A.12.1.3, HIPAA 164.312(b), PCI DSS 10.3.6, 11.5, GDPR Art. 32(1), COBIT DSS03.05, CCPA 1798.150(a)(1) |
| 7.2 **Goal:** Confirm a documented incident response plan is in place, regularly tested, and that security incidents are handled and resolved | * Implement and test an incident response process for security event detection and resolution | Security Lead, GRC Manager | * Incident Response Plan (IRP) document * Incident logs or Jira tickets showing resolution steps * Tabletop exercise report with findings and attendees * Post-incident review or root cause analysis * IR training completion records | COSO Principle 16, NIST CSF RS.AN-1, RS.CO-2, NIST SP 800-53 IR-4, IR-6, ISO A.16.1.1–16.1.5, HIPAA 164.308(a)(6)(ii), PCI DSS 12.10.1–12.10.6, GDPR Art. 33, COBIT DSS05.06, CCPA 1798.150(a)(1) |
| 7.3 **Goal:** Ensure the organization has a defined vulnerability management process that results in documented detection, prioritization, and remediation. | * Perform regular vulnerability scans and apply patches based on risk severity | Security Team, DevOps | * Vulnerability scan reports (e.g., Nessus, Qualys) * Patch management logs or tracking tickets * Risk scoring of vulnerabilities (CVSS or custom) * Documentation of applied patches or mitigations * Threat intelligence feed integrations (e.g., CISA, MISP) | COSO Principle 7, NIST CSF ID.RA-5, NIST SP 800-53 RA-5, SI-2, ISO A.12.6.1, HIPAA 164.308(a)(1)(ii)(A), PCI DSS 6.1, 11.2, GDPR Recital 83, COBIT DSS05.07, CCPA 1798.150(a)(1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC8.0 – CHANGE MANAGEMENT **Goal:** Ensure all changes to production systems are authorized, tested, and documented through a formal change management process, including retrospective review of emergency changes and safeguards to prevent unauthorized modifications. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 8.1 **Goal:** Confirm that all production changes are approved in advance and documented through a formal change management process.. | * Require formal approval for all system changes prior to deployment | Engineering Lead, DevOps, GRC | * Change request tickets (e.g., Jira) with approval history * Pull requests (PRs) showing reviewer comments and merge approvals * Change control policy outlining approval workflow * Risk assessment or rollback plan for significant changes | COSO Principle 10, NIST CSF PR.IP-3, NIST SP 800-53 CM-3, CM-5, ISO A.12.1.2, HIPAA 164.312(c)(1), PCI DSS 6.4.5, GDPR Art. 32, COBIT BAI06.01, CCPA 1798.100(b) |
| 8.2 **Goal:** Ensure changes are subject to pre-deployment testing and documented approval processes. | * Validate changes through testing and peer review before production release | Engineering Lead, QA, DevOps | * Jira or ServiceNow tickets with testing sign-off * Pull request (PR) with validation and reviewer notes * Unit, integration, or UAT test result logs * Change logs indicating successful deployment and rollback readiness | COSO Principle 11, NIST CSF PR.IP-2, NIST SP 800-53 SA-11, CM-4, ISO A.14.2.9, HIPAA 164.308(a)(8), PCI DSS 6.4.4, GDPR Art. 32, COBIT BAI06.03, CCPA 1798.105(c) |
| 8.3 **Goal:** Verify that urgent changes are tracked, approved retrospectively, and assessed for risk and control impact. | * Document and review emergency changes with post-implementation analysis | Engineering Lead, GRC | * Emergency change tickets with after-the-fact approvals * Change logs indicating incident-related modifications * Post-change impact analysis or root cause review * IRP reference documenting process for emergency changes | COSO Principle 11, NIST CSF PR.IP-9, NIST SP 800-53 CM-3(2), IR-4(3), ISO A.12.1.2, HIPAA 164.308(a)(6)(ii), PCI DSS 6.4.6, GDPR Art. 32, COBIT BAI06.06, CCPA 1798.150(a)(1) |
| 8.4 **Goal:** Confirm that changes to production systems are controlled and cannot be made without appropriate approvals. | * Restrict change access to authorized personnel and monitor unauthorized changes | DevOps, Security Team | * Change control policy outlining approval paths * Access control logs limiting deployment permissions * GitHub/GitLab role settings preventing unauthorized merges * Screenshots showing CI/CD or infrastructure-as-code enforcement * Review logs for unapproved changes or anomalies | COSO Principle 11, NIST CSF PR.AC-5, NIST SP 800-53 CM-5, AC-6(9), ISO A.12.5.1, HIPAA 164.312(c)(1), PCI DSS 10.2.7, 6.4.5, GDPR Art. 32, COBIT DSS05.01, CCPA 1798.150(a)(1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC9.0 – RISK MITIGATION **Goal:** Ensure the organization identifies, evaluates, and mitigates vendor and external risks through formal onboarding assessments, continuous tracking, and adaptation to emerging threats based on updated intelligence and oversight. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 9.1 **Goal:** Confirm that vendor risk is assessed, documented, and considered during onboarding and periodically thereafter. | * Evaluate risks associated with vendors and third parties before onboarding | GRC Lead, Legal, Procurement | * Vendor risk questionnaire or due diligence form * Copy of vendor SOC 2 / ISO 27001 reports * Risk rating spreadsheet or tracker * Approved vendor list with risk tiering * Vendor management policy referencing evaluation criteria | COSO Principle 15, NIST CSF ID.SC-3, NIST SP 800-53 SR-2, SR-3, ISO A.15.1.1, HIPAA 164.308(b)(1), PCI DSS 12.8.1–12.8.2, GDPR Art. 28(1), COBIT APO10.02, CCPA 1798.140(w) |
| 9.2 **Goal:** Demonstrate that vendor risks are actively tracked and remediated based on impact, with evidence of oversight. | * Remediate vendor risk findings and track issues until resolution | GRC Lead, Vendor Manager | * Vendor risk mitigation plans or follow-up logs * Notes from security or risk review meetings * Updated vendor risk ratings after control validation * Remediation evidence (e.g., contract updates, encryption enabled) * Approved exceptions with documented justification | COSO Principle 15, NIST CSF ID.SC-4, NIST SP 800-53 SR-5, SR-6, ISO A.15.1.2, HIPAA 164.308(b)(4), PCI DSS 12.8.3, GDPR Art. 28(3), COBIT APO10.03, CCPA 1798.100(d) |
| 9.3 **Goal:** Demonstrate that the organization stays current with threat intelligence and adapts its security posture accordingly. | * Monitor emerging risks and threats and adapt controls accordingly | Security Lead, GRC, CTO | * Subscriptions to threat intelligence feeds (e.g., CISA, MISP) * Patch or mitigation actions triggered by zero-day vulnerabilities * Updated risk register entries in response to new threats * Email advisories or meeting notes related to emerging threats * Change management tickets with associated security updates | COSO Principle 9, NIST CSF ID.RA-5, NIST SP 800-53 RA-5(2), PM-16, ISO A.6.1.3, HIPAA 164.308(a)(1)(ii)(A), PCI DSS 6.1, GDPR Art. 35, COBIT APO12.06, CCPA 1798.150(a)(1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A1.0 – AVAILABILITY (OPTIONAL) **Goal:** Ensure the organization defines and monitors system availability objectives, evaluates and mitigates related risks, and maintains tested backup and recovery procedures to support business continuity and service reliability. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 1.1 **Goal:** Confirm that system availability targets are defined, monitored, and supported by documented controls and testing. | * Define and document system availability goals and SLAs | CTO, Product Manager, Engineering | * SLA with uptime and RTO/RPO targets * Performance monitoring dashboards (e.g., Datadog, New Relic) * Capacity planning reports or architectural diagrams * Availability policy or system availability plan * Logs or records of availability-related alerts and responses | COSO Principle 13, NIST CSF PR.PT-5, NIST SP 800-53 CP-2, CP-6, CP-7, ISO A.17.1.2, HIPAA 164.308(a)(7), PCI DSS 12.10.6, GDPR Recital 49, COBIT DSS04.01, CCPA 1798.150(a)(1) |
| 1.2 **Goal:** Demonstrate that availability-related risks are documented, reviewed, and mitigated as part of the risk management program. | * Identify and assess risks that could affect system uptime or availability | GRC, Engineering, Security | * Availability section in enterprise risk assessment * Capacity planning reports (CPU, memory, bandwidth trends) * Business impact analysis (BIA) * Risk treatment plans or mitigation tickets * Availability threat modeling documentation | COSO Principle 7, NIST CSF ID.BE-5, NIST SP 800-53 RA-3, CP-9, ISO A.17.1.1, HIPAA 164.308(a)(7)(ii)(B), PCI DSS 12.1.3, GDPR Art. 32, COBIT APO12.03, CCPA 1798.100(d) |
| 1.3 **Goal:** Demonstrate that backups are scheduled, verified, and restorable, and that recovery processes are documented and tested. | * Implement and test backup and disaster recovery procedures | DevOps, Security, GRC | * Automated backup configuration screenshots * Backup success/failure logs and alerts * Recovery test reports (e.g., database restore) * Business continuity and DR test documentation * RTO (Recovery Time Objective) / RPO (Recovery Point Objective) policies | COSO Principle 17, NIST CSF PR.IP-4, PR.IP-9, NIST SP 800-53 CP-4, CP-6, CP-10, ISO A.12.3.1, A.17.1.3, HIPAA 164.308(a)(7)(ii)(C), PCI DSS 9.5.1, 12.10.6, GDPR Art. 32(1)(c), COBIT DSS04.03, CCPA 1798.150(a)(1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| C1.0 – CONFIDENTIALITY (OPTIONAL) **Goal:** Ensure that confidential information is clearly identified and classified, protected through encryption and access controls both in transit and at rest, reviewed regularly for authorized access, and disposed of securely and irreversibly when no longer needed. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 1.1 **Goal:** Confirm that confidential data types are defined, classified, and mapped to appropriate handling procedures. | * Identify and classify confidential data across systems and environments | GRC, Data Owner, Security | * Data classification policy or schema * Confidentiality labeling on documents or systems * Data inventory with classification tags * Policy mapping access or protection controls by classification * List of restricted/confidential data assets | COSO Principle 13, NIST CSF ID.AM-5, NIST SP 800-53 PL-2, MP-3, ISO A.8.2.1, HIPAA 164.312(a)(1), PCI DSS 3.1, GDPR Art. 30, COBIT DSS06.02, CCPA 1798.140(o)(1) |
| 1.2 **Goal:** Ensure that only authorized personnel have access to confidential data and that access is reviewed and logged. | * Restrict access to confidential data using technical and administrative safeguards | DevOps, IT Admin, Security | * Access control policy aligned with data classification * IAM role and group mapping for restricted/confidential data * Access review logs for data repositories or storage systems * Screenshots showing restricted access folders or databases * Audit trails showing access activity and permissions | COSO Principle 10, NIST CSF PR.AC-4, NIST SP 800-53 AC-3, AC-6, MP-5, ISO A.9.1.2, HIPAA 164.312(a)(1), PCI DSS 7.1.1, 7.2, GDPR Art. 32(1)(b), COBIT DSS05.04, CCPA 1798.105(c) |
| 1.3 **Goal:** Confirm data in transit is encrypted using strong protocols and that controls are documented and enforced. | * Protect confidential data in transit using secure protocols | Engineering, Security | * TLS/HTTPS configuration screenshots for applications * Network architecture diagram showing encryption layers * Encryption policy for data in transit * Third-party tools demonstrating encrypted transmissions (e.g., Wireshark output) * Configuration files enforcing secure transport protocols (e.g., SMTP/TLS, SFTP) | COSO Principle 10, NIST CSF PR.DS-2, NIST SP 800-53 SC-12, SC-13, SC-28(1), ISO A.13.2.3, HIPAA 164.312(e)(1), PCI DSS 4.1, 4.2, GDPR Art. 32(1), COBIT DSS05.01, CCPA 1798.150(a)(1) |
| 1.4 **Goal:** Confirm that confidential data is encrypted or otherwise protected at rest and that only authorized personnel can access it. | * Protect confidential data at rest with encryption and access controls | DevOps, Security, IT | * Storage encryption configurations (e.g., AWS KMS, Azure Storage) * Access control policies for storage systems * Evidence of full-disk encryption on endpoints * Encryption key management policy * Screenshots of database or file system encryption status | COSO Principle 10, NIST CSF PR.DS-1, NIST SP 800-53 SC-28, SC-12, ISO A.10.1.1, HIPAA 164.312(c)(1), PCI DSS 3.4, GDPR Art. 32, COBIT DSS05.01, CCPA 1798.150(a)(1) |
| 1.5 **Goal:** Verify that disposal of confidential data is documented, secure, and irreversible. | * Securely dispose of confidential data and media when no longer needed | IT Admin, GRC | * Data disposal or retention policy * Certificates of destruction from vendors * Logs of deleted records or secure wipe software output * Screenshots of automated expiration or retention rules * Disposal sign-off sheets or approval workflows | COSO Principle 10, NIST CSF PR.IP-6, NIST SP 800-53 MP-6, ISO A.8.3.2, A.11.2.7, HIPAA 164.310(d)(2), PCI DSS 9.8.2, GDPR Art. 17, COBIT DSS05.08, CCPA 1798.105(c) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PI1.0 – PROCESSING INTEGRITY (OPTIONAL) **Goal:** Ensure that systems process data accurately, completely, and as intended by implementing validation controls, detecting errors through automated and manual checks, and reviewing outputs regularly to identify and correct anomalies. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 1.1 **Goal:** Confirm that business and system processes are working as designed and produce accurate outputs without unauthorized manipulation. | * Ensure system processing is complete, accurate, timely, and authorized | Engineering, QA, Product | * Application input/output validation logs * Automated reconciliation reports * QA test plans and results * Transaction processing rules and exceptions * Logging of failed or incomplete transactions | COSO Principle 11, NIST CSF PR.DS-6, NIST SP 800-53 SI-7, AU-6(1), ISO A.12.2.1, A.14.1.3, HIPAA 164.312(c)(1), PCI DSS 6.5.1, 10.3.5, GDPR Art. 5(1)(d), COBIT DSS06.06, CCPA 1798.105(c) |
| 1.2 **Goal:** Demonstrate that automated and manual checks are in place to prevent and detect processing errors. | * Validate system inputs and outputs through automated or manual checks | QA Lead, DevOps, Engineering | * Input validation rules in application code or form logic * Logging of rejected or malformed inputs * Output validation scripts or reconciliation reports * Evidence of exception handling and alerts * Screenshots from QA/test environments showing validation workflows | COSO Principle 11, NIST CSF PR.IP-1, NIST SP 800-53 SI-10, SI-11, ISO A.14.1.2, HIPAA 164.312(c)(1), PCI DSS 6.5.1–6.5.2, GDPR Art. 5(1)(d), COBIT BAI03.05, CCPA 1798.105(c) |
| 3.0 **Goal:** Verify that output results are regularly reviewed, anomalies are investigated, and corrective actions are taken. | * Reconcile processing results to identify and correct discrepancies | QA, Product, GRC | * Output reconciliation logs or exception reports * Sign-off on financial or operational reports * Comparison reports (input vs. output summaries) * Workflow audit trails showing post-processing review * Root cause analysis of discrepancies | COSO Principle 3, NIST SP 800-53 PM-3, ISO A.5.3.2, HIPAA 164.308(a)(3) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P1.0–P9.0 – PRIVACY (OPTIONAL) **Goal:** Ensure the organization transparently communicates privacy practices, honors consent and access rights, collects only necessary data, enforces retention and deletion policies, protects personal data with technical and administrative safeguards, shares information responsibly, maintains data accuracy, and regularly monitors and enforces compliance with privacy requirements. | | | | |
| **STEP** | **ACTION** | **RESPONSIBLE PARTY** | **EXAMPLE EVIDENCE** | **MAPPED FRAMEWORKS** |
| 1.0 **Goal:** Verify that privacy notices are up to date, clearly written, and made available before or at the point of data collection. | * Publish and maintain an accurate, accessible privacy notice | Legal, GRC, Marketing | * Published privacy policy on website or app * Version history of privacy notice updates * Consent banner with links to privacy notice * Documentation showing when and how individuals are informed * Translations or adaptations for relevant user segments | COSO Principle 13, NIST CSF PR.PT-1, NIST SP 800-53 AR-1, TR-1, ISO 27701 7.3.1, HIPAA 164.520, GDPR Art. 13, COBIT APO13.02, CCPA 1798.100(b) |
| 2.0 **Goal:** Confirm consent is collected when necessary, documented, and tracked with the ability to honor opt-in/opt-out preferences. | * Collect and track consent in accordance with legal and policy requirements | Product, Engineering, Legal | * Consent banners or pop-ups with action tracking * Screenshots or logs from consent management platform (CMP) * Consent withdrawal workflow documentation * Audit log of individual preference changes * Data flow diagram showing where consent is enforced | COSO Principle 8, NIST CSF PR.PT-2, NIST SP 800-53 AR-5, UL-1, ISO 27701 7.3.2, HIPAA 164.508, GDPR Art. 7, COBIT APO13.03, CCPA 1798.120(a) |
| 3.0 **Goal:** Demonstrate that data collection practices are purpose-driven, minimal, and aligned with documented use cases. | * Limit personal data collection to what is necessary for disclosed purposes | Product Manager, Engineering | * Data collection matrix mapping fields to purposes * Forms or UI screenshots with minimal required fields * Policy or procedure for data minimization * Audit logs showing rejected or restricted data fields * DPIA (Data Protection Impact Assessment) documenting justification for collection | COSO Principle 6, NIST CSF ID.AM-1, NIST SP 800-53 AP-1, DM-1, ISO 27701 7.4.1, HIPAA 164.502(b), GDPR Art. 5(1)(c), COBIT BAI03.01, CCPA 1798.100(b) |
| 4.0 **Goal:** Demonstrate alignment between data usage, retention periods, and secure deletion or destruction policies. | * Define data use, retention, and secure disposal practices | Legal, GRC, Engineering | * Retention and deletion policy aligned to data types * Automated retention schedules in cloud storage or database * Data minimization documentation in business processes * Deletion logs or system configurations (e.g., retention rules in SaaS platforms) * Proof of secure disposal (e.g., destruction certificates, wipe confirmations) | COSO Principle 10, NIST CSF PR.IP-6, NIST SP 800-53 DM-2, MP-6, ISO 27701 7.4.7, HIPAA 164.310(d)(2), PCI DSS 9.8.2, GDPR Art. 5(1)(e), 17, COBIT DSS06.05, CCPA 1798.105(c) |
| 5.0 **Goal:** Confirm that individuals can access their data and that requests are fulfilled securely and within required timeframes. | * Enable individuals to access, correct, and delete their personal data | GRC, Support, Legal | * Data Subject Access Request (DSAR) process documentation * DSAR tracking logs or ticketing system exports * Example redacted DSAR response * Identity verification procedures for request fulfillment * Automated tools or dashboards for subject access requests | COSO Principle 15, NIST CSF PR.AC-1, PR.PT-3, NIST SP 800-53 IR-9, ISO 27701 7.3.5, HIPAA 164.524, GDPR Art. 15, COBIT DSS05.04, CCPA 1798.100, 1798.110 |
| 6.0 **Goal:** Verify that data sharing with vendors or partners is documented, limited to necessity, and protected by contractual and technical controls. | * Limit third-party disclosures and monitor vendor privacy controls | Legal, Security, Procurement | * List of approved third-party data recipients * Data processing agreements (DPAs) or standard contractual clauses * Vendor due diligence assessments and risk scores * Data transfer logs or API usage monitoring * Policy language restricting third-party disclosures | COSO Principle 15, NIST CSF ID.SC-1, NIST SP 800-53 AR-3, SA-4, ISO 27701 7.4.4, HIPAA 164.502(e), GDPR Art. 28(3), COBIT APO10.03, CCPA 1798.115(a) |
| 7.0 **Goal:** Confirm that personal data is protected by technical and administrative controls aligned to privacy and security policies. | * Apply security safeguards to protect personal data | Security, IT, GRC | * Access control configurations (e.g., IAM roles, permissions) * Encryption settings for data in transit and at rest * Data loss prevention (DLP) tool configurations * Audit logs showing access to personal data * Privacy and security training records | COSO Principle 10, NIST CSF PR.DS-1–DS-5, NIST SP 800-53 SC-12–SC-28, AR-6, ISO 27701 6.10.1, HIPAA 164.312(a)-(c), GDPR Art. 32, COBIT DSS05, CCPA 1798.150(a)(1) |
| 8.0 **Goal:** Confirm that data input, processing, and maintenance procedures support data quality and allow for corrections when needed. | * Maintain personal data accuracy and provide update mechanisms | Product, QA, Support | * Data validation and cleansing procedures * User-facing tools for updating personal information * Audit trails showing changes to user records * Data quality metrics or exception reports * Internal policies on accuracy and completeness | COSO Principle 13, NIST CSF PR.IP-1, NIST SP 800-53 AR-4, ISO 27701 7.3.3, HIPAA 164.526, GDPR Art. 5(1)(d), COBIT MEA03.02, CCPA 1798.130(a)(3)(D) |
| 9.0 **Goal:** Demonstrate that privacy practices are regularly reviewed, enforced, and updated based on findings or complaints. | * Monitor and enforce privacy compliance through audits and remediation | GRC, Legal, Privacy Officer | * Privacy audit reports or internal assessments * Logs of privacy complaints and resolution * Disciplinary action records related to policy violations * Records of periodic policy reviews or updates * Privacy monitoring dashboard or KPIs | COSO Principle 17, NIST CSF RS.CO-1, NIST SP 800-53 AR-6, IR-7, ISO 27701 7.5.1, HIPAA 164.308(a)(1)(ii)(C), GDPR Art. 58, COBIT MEA02.01, CCPA 1798.135(a)(2) |

## FRAMEWORK REFERENCE SUMMARIES:

* **COSO (Committee of Sponsoring Organizations of the Treadway Commission)**

A framework for designing and evaluating internal controls over financial and operational reporting, consisting of 17 principles across five components: Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring.

* **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.