**STARTUP SECURITY ROADMAP (12-MONTH)**

***Building Trust, Readiness, and Resilience from Day One***

**Document Type:** Security Program Strategy & Implementation Guide  
**Audience:** Executive Team, Security Leadership, Product Stakeholders, Compliance Teams **Last Updated:** May 2025

This roadmap outlines a strategic 12-month plan for maturing a startup’s cybersecurity posture, with a phased approach that aligns security operations to business growth. Designed for high-growth B2B SaaS environments, the roadmap spans four key phases—Baseline, Harden, Automate, and Monitor—to help teams operationalize compliance, reduce security risk, and prepare for external audits.

Each phase includes clear milestones, assigned responsibilities, helpful tools, required deliverables, and mapped references to leading frameworks including ISO/IEC 27001:2022, NIST CSF, NIST SP 800 series, HIPAA, PCI DSS, GDPR, CCPA, COBIT, and COSO.

Whether preparing for SOC 2 Type II, ISO certification, or HIPAA alignment, this roadmap ensures your startup is not only secure—but provably so.

This document supports strategic security planning, foundational team enablement, and repeatable audit readiness to accelerate customer trust, scale governance, and build a security-first culture.

**TABLE OF CONTENTS:**

[Phase 1: BASELINE (Month 1–3) 2](#_Toc197259625)

[Phase 2: HARDEN (Month 4–6) 3](#_Toc197259626)

[Phase 3: AUTOMATE (Month 7–9) 4](#_Toc197259627)

[Phase 4: MONITOR (Month 10–12) 5](#_Toc197259628)

## Phase 1: BASELINE (Month 1–3)

**Objective:** Establish foundational security practices, identify risks, and initiate compliance alignment.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Step** | **Initiative** | **Responsible Party** | **Tools & Services** | **Deliverable** | **Framework Mappings** |
| 1.1 Asset Inventory & Data Mapping | * Identify cloud/infrastructure assets, SaaS tools, data types. * Classify sensitive data (PII, PHI). * Build a system/data flow diagram. | Engineering + Security | CMDB (ServiceNow, AssetTiger), AWS Config, Spreadsheet tracker | * Updated asset register * Data flow map * Classification matrix | ISO 27001 A.5, NIST CSF ID.AM, GDPR Art. 30 |
| 1.2 Initial Risk Assessment | * Identify internal/external risks. * Calculate likelihood/impact. * Rank by risk level. | GRC + Founders | Risk register template, STRIDE, Threat modeling software (ThreatModeler) | * Risk Register with mitigation plans. | NIST SP 800-30, ISO 27005, COSO |
| 1.3 Minimum Viable Security Policies | * Customize templates to fit team structure and tech stack. * Require acknowledgment via HR/onboarding. | Security Lead | Google Workspace, Notion | * Signed policies: Acceptable Use, Access Control, Incident Response, Data Classification | ISO 27001 A.5, A.9, HIPAA §164.308, COBIT APO13 |
| 1.4 Role-Based Access Control (RBAC) | * Define roles and permissions per job function. * Remove shared accounts. * Enforce least privilege. | Engineering + Security | AWS IAM, Okta, Google Workspace, JumpCloud | * IAM matrix * Access control SOP * Access audit report | ISO 27001 A.9, NIST SP 800-53 AC-2, PCI DSS 7 |
| 1.5 Vendor Risk Management | * List all third-party vendors. * Assess security posture (SOC 2, ISO 27001 certs). * Review DPAs and SLAs. | Legal + Security | Vendor assessment questionnaire, OneTrust, Spreadsheet tracker | * Vendor assessment report (SOC2, ISO 27001) * Due diligence documentation | GDPR Art. 28, ISO 27001 A.15, NIST CSF ID.SC |
| 1.6 Compliance Path Selection | * Evaluate customer expectations and vertical (e.g., SOC 2 for SaaS, HIPAA for healthcare). * Review overlap between frameworks. | CEO + Security Advisor |  | * Milestone plan * Early gap assessment | CCPA §1798.100+, ISO 27001 clause 4, SOC 2 TSC |

## Phase 2: HARDEN (Month 4–6)

**Objective:** Strengthen defenses through secure configuration, training, and formal controls.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Step** | **Initiative** | **Responsible Party** | **Tools & Services** | **Deliverable** | **Framework Mappings** |
| 2.1 Secure Configurations | * Harden cloud workloads. * Disable unused services. * Secure containers. * Enforce password policies. | DevOps + Security | CIS Benchmarks, AWS Config, Ansible | * Hardened system baselines * Screenshots/config file archive * CIS Benchmark reports | NIST SP 800-53 CM-2, ISO 27001 A.12, PCI DSS 2.2 |
| 2.2 MFA, SSO Implementation | * Enforce MFA on all systems. * Implement SSO for central auth. * Disable legacy auth methods. | IT + Engineering | Okta, Google Workspace, Duo, Azure AD | * MFA enforcement report * User onboarding SOP | NIST CSF PR.AC, HIPAA §164.312(d), ISO A.9.4 |
| 2.3 Security Awareness Training | * Assign mandatory annual training. * Phishing simulations. * Onboarding training. * Track completions. | Security + HR | KnowBe4, Curricula, or free options like SANS security awareness videos | * Training completion logs * Phishing sim results | ISO 27001 A.7.2.2, NIST SP 800-50, HIPAA §164.308(a)(5) |
| 2.4 Vulnerability Management | * Scan infra and dependencies, prioritize based on CVSS. * Create patch schedule with DevOps. | Security + DevOps | Nessus, OpenVAS, AWS Inspector, GitHub Dependabot | * Monthly scan reports * Patching evidence logs | NIST SP 800-40, PCI DSS 6.2, COBIT DSS05 |
| 2.5 Backup and Recovery | * Define RTO/RPO * Test restore from backups quarterly * Encrypt backups | DevOps | AWS Backup, Veeam, GitHub snapshotting | * Backup logs * Test results * Documented BCP/DRP * RTO/RPO metrics | ISO 27001 A.17, NIST SP 800-34, HIPAA §164.308(a)(7) |
| 2.6 Draft SoA (if pursuing ISO) | * Identify applicable Annex A controls * Document justification for inclusions/exclusions | GRC |  | * Draft Statement of Applicability stored in audit folder | ISO 27001 clause 6.1.3, SOC 2 |

## Phase 3: AUTOMATE (Month 7–9)

**Objective:** Reduce manual overhead, improve auditability, and prepare for certification.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Step** | **Initiative** | **Responsible Party** | **Tools & Services** | **Deliverable** | **Framework Mappings** |
| 3.1 Infrastructure-as-Code (IaC) Security | * Secure infrastructure modules with guardrails, version control for infrastructure. | DevOps + Engineering | Terraform, CloudFormation, tfsec, Checkov | * Reviewed IaC modules with security annotations * Policy-as-code rules | ISO A.12.1.2, NIST SP 800-53 SC-12, COBIT BAI03 |
| 3.2 Centralized Logging + Alerting | * Enable log ingestion from servers, endpoints, SaaS apps. * Set alert rules for unauthorized access, privilege escalation, etc. | Security | ELK Stack, Datadog, AWS CloudTrail + CloudWatch, Panther | * Audit log retention strategy * Alert dashboard | NIST CSF DE.CM, PCI DSS 10.5, ISO A.12.4 |
| 3.3 Endpoint Detection & Response (EDR) | * Deploy EDR agent to all devices. * Configure rules for common threats. * Enable auto-containment. | Security + IT | CrowdStrike, SentinelOne, Microsoft Defender | * Deployment map * Detection rules | NIST SP 800-53 SI-4, HIPAA §164.308(a)(1)(ii)(A) |
| 3.4 Compliance Automation Platform | * Connect systems (HRIS, AWS, GDrive). * Track controls. * Prepare evidence collection workflow. | Security + GRC | Drata, Vanta, Secureframe, Tugboat Logic | * Automated control dashboard * Audit-ready file vault | SOC 2 CC1–CC5, ISO 27001 clause 9, NIST CSF ID.GV |
| 3.5 SLAs for Security Functions | * Define SLAs for vulnerability remediation, incident response, and user onboarding/offboarding. | Product + Security |  | * SLA documents signed off by leadership and security | ISO 27001 A.14, NIST SP 800-53 CP-10 |
| 3.6 Mock Audit Prep | * Conduct internal walkthroughs of control evidence. * Identify gaps. * Create CAPA (Corrective Action & Preventive Action) plans. | GRC |  | * Mock audit report * Gap remediation tracker | SOC 2 TSC, ISO 27001 audit clause 9, PCI DSS ROC prep |

## Phase 4: MONITOR (Month 10–12)

**Objective:** Mature into continuous security monitoring, incident response, and improvement cycles.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Step** | **Initiative** | **Responsible Party** | **Tools & Services** | **Deliverable** | **Framework Mappings** |
| 4.1 Incident Response Plan Testing | * Simulate breach scenario. * Log response timeline. * Identify IR gaps. | Security + Executive Team | IR playbook, tabletop template | * IR plan updated with lessons learned * IR test report * Tabletop exercise log | ISO A.16, NIST SP 800-61, HIPAA §164.308(a)(6) |
| 4.2 Threat Intelligence Integration | * Review threat actor TTPs. * Update detection rules. * Align with MITRE ATT&CK. | Security | OpenCTI, MISP, commercial feeds | * Threat model update * IOC watchlist * Tuning history | NIST CSF DE.AE, COBIT DSS04, ISO A.12.6 |
| 4.3 Security Metrics & KPIs | * Metrics include: MTTR, user awareness score, endpoint coverage, and control coverage. | Security + CEO | Excel dashboard, Tableau, compliance automation reports | * Executive-level dashboard shared monthly: incidents, coverage, risk scores | COSO, CCPA, ISO clause 10.1 |
| 4.4 Internal Audit & Mgmt Review | * Conduct internal audit using ISO/PCI templates. * Host review with senior leadership. * Track improvements. | GRC + Executive Team |  | * Audit findings * Management response plan * Continuous improvement log | ISO 27001 clause 9, SOC 2 review cycle |
| 4.5 External Audit or Certification | * Engage auditor (SOC 2 firm, ISO registrar) * Finalize SoA and Evidence folder. | GRC + Security |  | * OC 2 Type I/II report or ISO certificate | Depends on selected path |