WHITE PAPER

Building a Security Program from Scratch

A Practical Roadmap for Startups and Growing Organizations

How to build a pragmatic, compliance-ready security program from the ground up — covering governance, access control, vulnerability management, incident response, and the path to SOC 2, ISO 27001, and other key frameworks.

Version 1.0

Prepared By Lorikeet Security

lorikeetsecurity.com

OVERVIEW

1. Introduction

Most startups treat security as something they'll deal with later — after the product ships, after the first enterprise deal, after the breach. The organizations that build security programs early consistently emerge with lower remediation costs, faster enterprise sales cycles, and better cyber insurance positioning than those that bolt it on after the fact.

This whitepaper provides a practical, phased roadmap for building a security program from scratch — one that's right-sized for where you are today, scales as you grow, and maps to the compliance frameworks enterprise customers will require.

> **Start Here**
>
> You don't need to do everything at once. A security program is built in phases. The goal of Phase 1 is not perfection — it's a defensible baseline that reduces your most significant risks and positions you to achieve SOC 2 within 6–12 months.

FOUNDATIONS

2. Phase 1: Foundations (Month 1–2)

The foundation of any security program is governance: defining who owns security, what you're protecting, and what your baseline policies are. These activities cost little but provide the structural scaffolding everything else builds on.

Action	Description	Output
Assign Security Ownership	Designate a security owner (CTO, vCISO, or security lead). This person owns the program, drives accountability, and interfaces with auditors.	Named security owner with defined responsibilities.
Define Your Asset Inventory	Document all systems, data stores, cloud environments, and third-party integrations. You can't protect what you haven't enumerated.	Asset inventory spreadsheet or CMDB.
Classify Your Data	Define data sensitivity tiers (e.g., Public, Internal, Confidential, Restricted) and identify where each type lives. Map PII, PHI, and cardholder data explicitly.	Data classification policy and data map.

Action	Description	Output
Write Core Security Policies	Start with: Acceptable Use, Access Control, Incident Response, Password Policy, and Vendor Management. Templates are available; customize for your context.	Policy library (5–10 documents).
Conduct a Risk Assessment	Identify your top 10 risks based on asset inventory and data map. Rate each by likelihood and impact. This is required by SOC 2, ISO 27001, and most other frameworks.	Risk register with treatment decisions.

ACCESS & IDENTITY

3. Phase 2: Access Control and Identity (Month 2–3)

The majority of breaches involve compromised credentials or excessive access. Identity and access management (IAM) is the highest-ROI security control category for most organizations.

- Deploy Single Sign-On (SSO): Centralize authentication through an IdP (Okta, Google Workspace, Azure AD). SSO enables MFA enforcement and access revocation at offboarding.
- Enforce MFA everywhere: Require MFA on all systems — not just production, but also admin consoles, cloud portals, source code repositories, and communication tools.
- Implement least privilege: Audit current access grants. Remove dormant accounts. Restrict service accounts to minimum required permissions. Separate production access from development.
- Automate offboarding: Ensure employee and contractor offboarding triggers immediate access revocation across all systems. This is a frequent SOC 2 finding when done manually.
- Deploy a Privileged Access Management (PAM) solution: For organizations with sensitive infrastructure, tools like 1Password Business or CyberArk manage privileged credentials and provide an audit trail.
- Conduct quarterly access reviews: Review and re-certify user access grants every quarter. Document the reviews — auditors require evidence of this process.

VULNERABILITY MGMT

4. Phase 3: Vulnerability Management (Month 3–4)

Vulnerability management is the systematic process of identifying, prioritizing, and remediating security weaknesses across your environment. It is required by virtually every compliance framework.

Activity	Frequency	Tool / Approach
External Vulnerability Scanning	Weekly / Monthly	Nessus, Qualys, or Lorikeet's ASM platform for continuous external attack surface monitoring.

Activity	Frequency	Tool / Approach
Internal Vulnerability Scanning	Monthly	Nessus, OpenVAS, or Tenable.io for internal host scanning.
Web Application Scanning	Per-release + weekly	OWASP ZAP, Burp Suite Pro (automated), or Lorikeet's web security scanner for continuous baseline detection.
Software Composition Analysis (SCA)	Per-commit (CI/CD)	Snyk, OWASP Dependency-Check, or GitHub Dependabot for third-party library CVE detection.
Static Application Security Testing (SAST)	Per-commit (CI/CD)	Semgrep, CodeQL, or Checkmarx for source code vulnerability scanning.
Annual Penetration Test	Annual	Lorikeet Security manual penetration test. Provides compliance evidence and attack chain validation beyond what scanners detect.

MONITORING

5. Phase 4: Logging and Monitoring (Month 4–5)

You cannot respond to what you cannot see. Logging and monitoring capabilities are required by SOC 2 (CC7), ISO 27001 (Control 8.15), PCI DSS (Requirement 10), and HIPAA.

- Centralize logs: Deploy a SIEM or log aggregation platform (Splunk, Datadog, Elastic, or AWS CloudWatch). Collect logs from all infrastructure, applications, and cloud services.
- Define what to log: At minimum — all authentication events (success and failure), privilege escalation, administrative actions, data access on sensitive resources, and network connections.
- Set retention: Retain logs for a minimum of 12 months with at least 3 months immediately accessible. PCI DSS requires 12 months minimum.
- Create alerts for critical events: Failed login brute force patterns, after-hours admin access, privilege escalation, new admin account creation, and data export from sensitive systems.
- Enable cloud provider logging: AWS CloudTrail (all regions), VPC Flow Logs, S3 access logs. Azure Activity Log and Diagnostic Settings. GCP Cloud Audit Logs.
- Test your monitoring: Penetration testing findings are often the first indicator that logging and alerting is insufficient — use them to improve your detection capabilities.

INCIDENT RESPONSE

6. Phase 5: Incident Response (Month 5–6)

Component	Description
IR Policy	Define what constitutes a security incident, who is responsible for declaring one, and the escalation path. Include legal, PR, and executive contacts.
Incident Playbooks	Develop response playbooks for your most likely scenarios: ransomware, phishing / credential compromise, data breach / exfiltration, and cloud account compromise.
Communication Plan	Define internal and external communication templates. Include customer notification language for breach scenarios. Understand your regulatory notification timelines (GDPR: 72 hours; HIPAA: 60 days).
Tabletop Exercises	Conduct at least one tabletop exercise annually simulating a realistic incident scenario. Involve leadership, legal, and operations — not just the security team.
Forensic Readiness	Ensure you have access to a forensic investigation partner (Lorikeet Security provides incident response services). Preserve an offline backup of critical system images.
Post-Incident Review	Document and review every incident. Track root cause, detection time, response time, and remediation. Use findings to improve controls and playbooks.

COMPLIANCE ROADMAP

7. Mapping to Compliance Frameworks

Once your foundational program is in place, aligning to a compliance framework becomes significantly more efficient. The groundwork laid in Phases 1–5 maps directly to the controls required by major frameworks.

Framework	When to Target	Key Controls Covered by Your Program
SOC 2 Type I	Month 6–9	CC1 (governance), CC2 (communication), CC3 (risk assessment), CC6 (access control), CC8 (change management).
SOC 2 Type II	Month 12–18	All CC controls with 6–12 months of operating evidence. Requires demonstrated logging, incident response, and access reviews.
ISO/IEC 27001	Month 12–18	ISMS design, risk treatment, Annex A controls (organizational, people, physical, technological). Builds on your policy library and risk register.
PCI DSS v4.0	As needed for payment	Req. 7 (access control), Req. 8 (authentication), Req. 10 (logging), Req. 11 (penetration testing), Req. 12 (policy).

Framework	When to Target	Key Controls Covered by Your Program
HIPAA Security Rule	As needed for healthcare	Administrative safeguards (risk analysis, training, IR), Technical safeguards (access control, audit controls, encryption).
CMMC Level 2	As needed for DoD	110 NIST SP 800-171 practices across 14 domains. Multi-factor authentication, access control, and incident response are core.

TOOLS

8. Recommended Security Program Toolstack

Category	Recommended Tools	Notes
Identity / SSO / MFA	Okta, Google Workspace, Azure AD + FIDO2 keys	SSO is the highest-ROI security investment for most growing companies.
Secrets Management	HashiCorp Vault, AWS Secrets Manager, 1Password Business	Eliminates hardcoded credentials — a top pentest finding.
Vulnerability Scanning	Lorikeet ASM, Nessus, Qualys	Continuous external ASM + periodic internal scanning.
SAST / SCA	Semgrep, Snyk, GitHub Advanced Security	Shift-left scanning integrated into CI/CD pipelines.
SIEM / Logging	Datadog, Splunk, Elastic, AWS CloudWatch	Centralized log aggregation with alerting.
CSPM (Cloud Security)	Wiz, Prisma Cloud, AWS Security Hub	Continuous cloud misconfiguration detection.
Compliance Automation	Vanta, Drata (Lorikeet is partner of both)	Automates evidence collection for SOC 2, ISO 27001, and other frameworks.
Penetration Testing	Lorikeet Security	Annual manual testing plus ongoing ASM for continuous attack surface visibility.

HOW WE HELP

9. How Lorikeet Security Supports Your Program

Lorikeet Security is built for organizations at every stage of their security journey — from startups running their first penetration test to mature organizations seeking SOC 2 Type II attestation and ongoing managed security services.

Service	Description
Penetration Testing	Web app, API, network, cloud, mobile, and AI agent testing. Annual engagements with compliance-mapped reports and free retests.
Attack Surface Management	Continuous external asset discovery, subdomain enumeration, and automated vulnerability monitoring via the Lorikeet ASM platform.
vCISO / Security Advisory	Fractional CISO services to design your security program, build policies, manage compliance roadmaps, and advise the board.
Vulnerability Management	Managed vulnerability scanning, triage, and remediation tracking integrated with your development workflows.
SOC 2 Bundle	Penetration testing + audit attestation through our partner Accorp Partners CPA. One intake call, unified timeline.
Compliance Center	GRC platform integration with Vanta and Drata for automated evidence collection and continuous compliance monitoring.

Start Building Your Security Program Today

Contact Lorikeet Security at lorikeetsecurity.com or call (689) 202-3940 to discuss building or maturing your security program. Free scoping session, proposal within 24 hours.