Vulnerability Management Program

Policy Draft & Implementation Report

Author: Dan Chui

Target Role: GRC / Technology Risk / Security Governance

Date: March 2026

Environment: Simulated Enterprise Environment

1. Purpose

This document defines the structure, governance framework, and operational workflow for establishing a formal Vulnerability Management Program within a mid-sized enterprise environment. The objective is to ensure systematic identification, assessment, prioritization, remediation, and reporting of security vulnerabilities across organizational assets.

The program is designed to achieve:

- • Risk-based vulnerability prioritization
- • Defined remediation ownership and accountability
- • Measurable remediation timelines (SLA-driven)
- • Executive visibility into security risk posture
- • Continuous improvement through monitoring and reporting

2. Organizational Scope

- • Organization size: ~500 users
- • Hybrid infrastructure (on-prem + cloud workloads)
- • Centralized vulnerability scanning solution
- • Asset inventory maintained via CMDB
- • Security and IT Operations collaboration model

3. Governance & Roles

Program Owner: Security Governance / GRC Lead

Responsible for policy approval, reporting, and executive updates.

- Operational Owner: Vulnerability Management Lead
- Asset Owners: Responsible for remediation within SLA
- IT Operations: Executes patching and configuration updates
- Executive Management: Receives quarterly risk posture reports

4. Vulnerability Management Lifecycle

4.1 Identification

- • Authenticated vulnerability scans conducted on scheduled cadence
- • Coverage includes servers, endpoints, and network devices

4.2 Risk Classification

- • Severity based on CVSS score and exploitability
- • Business impact considered (critical systems prioritized)

Severity Levels:

- • Critical – Immediate business risk
- • High – Significant security exposure
- • Medium – Moderate risk requiring remediation
- • Low – Informational or minimal risk

4.3 Remediation & SLA

- • Critical: Remediation within 7 days
- • High: Remediation within 14 days
- • Medium: Remediation within 30 days
- • Low: Addressed during standard maintenance cycle

4.4 Validation

- • Follow-up scans confirm remediation effectiveness
- • Exceptions documented and formally approved

5. Program Outcomes (Initial Implementation Phase)

Initial Scan Findings:

- • Multiple outdated software versions detected
- • Weak configurations and unnecessary services identified
- • Privileged accounts lacking proper controls

Post-Remediation Results:

- • 100% of Critical vulnerabilities remediated
- • ~90% reduction in High-severity vulnerabilities
- • ~70% overall vulnerability count reduction

6. Reporting & Metrics

Key Metrics Tracked:

- • Total vulnerabilities by severity

- • Mean Time to Remediate (MTTR)
- • SLA compliance percentage
- • Risk trend analysis over time

Quarterly executive reporting includes summarized risk posture, trend analysis, and outstanding high-risk exposures.

7. Continuous Improvement & Maintenance Mode

- • Monthly scan cadence established
- • Policy review conducted annually
- • Integration with enterprise risk management reporting
- • Expansion to cloud-native assets and endpoints

8. Conclusion

The establishment of a structured Vulnerability Management Program significantly improves the organization's security posture through formal governance, risk-based prioritization, and measurable remediation accountability. This initiative demonstrates applied capability in policy development, cross-functional coordination, risk reporting, and operational security lifecycle management.