

Vulnerability Management Methodology

This methodology follows a systematic seven-phase approach to vulnerability management, creating a continuous cycle of security improvement. Each phase builds upon the previous one, ensuring comprehensive security coverage across the organization's IT infrastructure.

Phase 1: PREPARE

Define scope, identify assets, configure tools, establish responsibilities



Phase 2: IDENTIFY

Conduct vulnerability scans using OpenVAS and OWASP ZAP on all in-scope assets



Phase 3: ANALYZE

Review scan results, assign risk scores using risk matrix, create risk register



Phase 4: EVALUATE

Prioritize vulnerabilities based on business impact and likelihood of exploitation



Phase 5: RESPOND

Implement remediation strategies: patches, configuration changes, compensating controls



Phase 6: MONITOR

Conduct follow-up scans to verify remediation effectiveness and identify new issues



Phase 7: REPORT

Document findings, actions taken, outcomes, and recommendations for continuous improvement

Cycle Repeats

Key Principles

Continuous Cycle After reporting, the cycle returns to the Prepare phase for the next assessment period.	Risk-Based Prioritization Vulnerabilities are prioritized using the risk matrix that considers both business impact and likelihood of exploitation.
Proactive Security Regular scanning enables identification of vulnerabilities before they can be exploited and allows a proactive security approach.	Compensating Controls When direct remediation isn't possible, alternative security measures are implemented to mitigate risk.

Tools and Frameworks

Scanning Tools: OpenVAS (network and system vulnerabilities), OWASP ZAP (web application vulnerabilities)

Documentation: Microsoft Excel risk register and risk matrix for tracking and prioritization

Standards: NIST SP 800-30 (Risk Management), NIST SP 800-40 (Patch Management)

Access Method: SSH for secure remote management and remediation activities