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 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