

VA ENTERPRISE DESIGN PATTERNS INFORMATION TECHNOLOGY (IT) SERVICE MANAGEMENT VULNERABILITY MANAGEMENT



Office of Information and Technology

Version 1.0
February 2018

EXECUTIVE SUMMARY

Scope

This Enterprise Design Pattern (EDP) focuses on the process for identifying, classifying, remediating, and mitigating vulnerabilities found within Department of Veterans Affairs (VA) information technology (IT) infrastructure that is integral to both computer and network security. A robust Vulnerability Management (VM) program should be implemented within the enterprise in order to effectively remedy vulnerabilities identified in operating system (OS) databases, applications, and other network devices. This EDP makes recommendations for implementing standardized enterprise-wide VM practices that are based on industry best practices.

Topics that are out of scope for this EDP, but may be referenced, include the following:

- Configuration management and baselines
- Removing unauthorized software by removing user permissions and scanning
- Patch management
- Cloud computing

Business Need

Federal Information Security Management Act (FISMA) compliance, agency policy, and enterprise strategy are drivers for the following business needs at VA:

- A mature VM program that can resolve the FISMA audit findings
- Prioritization strategy, with enough granularity to account for the highest areas of risk when resources are limited
- An efficient VM program that minimizes risk exposure, while supporting service delivery
- A single strategy for the alignment of tools to the VM program; including removing tool overlap and resulting data conflicts, and integration with the Continuous Diagnostic and Mitigation (CDM) program
- A timely and reliable reporting that is based on authoritative data sources
- An authoritative source of IP address to system and system owner mapping

Approach

This EDP provides a vendor-agnostic approach to VM to support the discovery, prioritization, and remediation of vulnerabilities across the enterprise. The document will assist VA project teams, IT investment decision-makers, the Strategic Technology Alignment Team (STAT), and other stakeholders to identify issues associated with resolving FISMA audit and material weakness findings; and to make recommendations for program improvement. The EDP approach includes the following:

- Review existing capabilities and their limitations
- Analyze existing policy and governance
- Provide parameters for improving VM at VA

Enterprise Design Patterns (EDPs) are developed in coordination with internal and external subject matter experts and stakeholders. An EDP is a reusable capability guidance document that identifies best practice approaches and resources for achieving VA IT strategic objectives. The EDP Team uses industry trends and innovations; enterprise architectural standards; and guiding principles for capabilities and constraints to improve efficiency and effectiveness and define solutions to reoccurring technical problems. The EDP helps guide the design of IT systems and services by VA project teams.