



## What are Design Patterns?

Reusable templates that guide the enterprise to implement a set of technologies in standard ways

How do Design Patterns relate to the Enterprise?

Design Patterns translate OI&T's strategic goals, as documented in the Enterprise Technology Strategic Plan (ETSP), into "real world" direction to guide system design

How can I learn more?

To learn more about the ITSM Design Pattern, contact Nicholas Bogden (Nicholas.Bogden@va.gov)

To read the full document, see the TS website: [www.techstrategies.oit.va.gov](http://www.techstrategies.oit.va.gov)

To ask questions about Design Patterns in general, reach out to [askTS@va.gov](mailto:askTS@va.gov)

## Enterprise Design Patterns: IT Service Management (ITSM) Increment 1

- **Current State:** Recent Office of the Inspector General (OIG) audits noted VA has a material weakness in the configuration, change, patch, and vulnerability management areas of IT service management (ITSM)
- **Design Pattern Scope:** Addresses identified Federal Information System Controls Audit Manual (FISCAM) Audit Material Weaknesses
- **Design Pattern Solution:** Recommends an enterprise framework to create an end-to-end configuration management process, which will ultimately improve VA's security posture



Currently, there are efforts underway to implement a process to automate configuration, patch, and vulnerability management at the VA enterprise level.

Specifically, the ITSM design patterns responds to recent OIG, Federal Information Security Management Act (FISMA) and Federal Identity Credential and Access Management (FICAM) audits, which noted VA has a number of material weaknesses. Identified weaknesses span across the configuration, change, patch, and vulnerability management areas of IT service management (ITSM).

The first ITSM increment addresses two recommendations from VA's Continuous Readiness in Information Security Program (CRISP): Recommendation #1 and Recommendation #6

### 1. Recommendation #1: Vulnerability Discovery and Remediation

Implement a process to ensure all VA organizations are included in the vulnerability management program and implement improved mechanisms to continuously identify and remediate security deficiencies

### 2. Recommendation #6: Unauthorized Software Discovery and Remediation

Develop a comprehensive list of approved and unapproved software and implement a process for monitoring, preventing installation, and removing unauthorized application software on agency devices.

The design pattern will enable consistent enterprise-wide controls to support vulnerability management and IT asset management

These controls will be used to drive standardized development and operation of information systems. They will also include a formal, automated process for the identification and removal of unauthorized software to ensure proper accounting of approved IT assets in VA.

The design pattern was developed collaboratively with all OI&T pillars, as well as with representation from the Veterans Benefits Administration (VBA), Veterans Health Administration (VHA), and the National Cemetery Administration (NCA).

This will ultimately help VA decide which assets require changes and the level of impact of those changes. It will also allow VA to make informed information security, cost, and lifecycle-appropriate changes to a semi-automated process.