



What are Enterprise Design Patterns?

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

How do Enterprise Design Patterns relate to the Enterprise?

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 Mobile Enterprise Design Patterns, contact Joe Brooks (joseph.brooks2@va.gov)

To read the full document, see the TS website: www.techstrategies.oit.va.gov

To ask questions about Enterprise Design Patterns in general, reach out to AskTS@va.gov

Enterprise Design Patterns: Enterprise Auditing

- **Enterprise Design Pattern Scope:** VA has many applications in use by numerous users from various locations at any point in time. VA is responsible for monitoring use of IT resources to prevent misuse. VA Enterprise Auditing is the review of audit log data to determine the appropriateness of authentication, authorization, and access. Due to the volume of data and variety of sources, a solution is needed to manage the analysis of these logs in an efficient and effective manner. This solution is referred to as a Security Information and Event Management (SIEM) solution and is the primary focus of this Enterprise Design Pattern. This includes the collection and storage of audit events for use in security monitoring, trending, and reporting.
- **Current State:** This Enterprise Design Pattern establishes the official enterprise guideline for enterprise-wide auditing across all lines of business in accordance with Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) 800-53 and VA 6500 security policies (see Appendix D). Currently, NIST requires that VA must create, protect, and retain information system audit records needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. This approach ensures that the actions of individual information system users can be uniquely traced to those users, holding them accountable for their actions.

The VA Office of the Inspector General (OIG) also audits that VA consistently reviews security violations and audit logs supporting mission-critical systems each year. Recommendations were included in the last FISMA audit for VA to audit access logs and perform centralized reviews of security violations. Enhancements to VA's operational model described in this document will also provide the ability for business units across VA to perform security monitoring and analysis effectively for their area of responsibility.

VA currently has multiple solutions managed by separate groups that monitor a percentage of the available audit logs. The lack of an enterprise audit capability significantly increases VA's administrative burden and technology overhead; causing VA to manage multiple siloed, solutions which makes creating a comprehensive view of the enterprise very difficult. A lack of an adequate central repository for audit log retention also contributes to systems not generating or discarding events to preserve disk space on production assets.

- **Design Pattern Solution:** The Enterprise Auditing Design Pattern provides a vendor-agnostic SIEM framework that can be applied to VA's Enterprise IT Systems. The integration of this framework will require the following steps to take place:
 - Establish Governance
 - Systems Analysis
 - Systems Design
 - Implementation
 - Deployment
 - Maintenance

An Enterprise SIEM tool will have the ability to collect, aggregate, filter, and store security events for triage, correlation, trending, reporting, and compliance, offering both real time and historical analytics. The Enterprise Auditing solution will be an Enterprise Shared Service (ESS) that can support the business requirements of multiple stakeholders throughout VA requiring security event analytics and reporting. Older SIEM strategy focused on reducing events for analysis. New SIEM strategy focuses on including more events for analysis to provide context and relationships for deeper insights. A centralized data repository will enable this potential for all stakeholders.