VA Enterprise Design Patterns:

4. IT Service Management

4.4: ITSM Enterprise Framework

Office of Technology Strategies (TS)
Architecture, Strategy, and Design (ASD)
Office of Information and Technology (OI&T)

Version 0.7

Date Issued: November 2015

Draft

THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

Draft

APPROVAL COORDINATION

TIMOTHY L MCGRAIL 111224

Digitally signed by TIMOTHY L MCGRAIL 111224
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=tim.mcgrail@va.gov, cn=TIMOTHY L MCGRAIL 111224
Date: 2015.12.22 13:27:37 -05'00'

Date:

Tim McGrail
Senior Program Analyst
ASD Technology Strategies

PAUL A. TIBBITS 116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=paul.tibbits@va.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2015.12.22 14:26:53 -05'00'

Date:

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Organization	Notes
0.1	7/28/15	ASD TS	Initial draft outlining the business need, approach and current capabilities
0.3	8/20/15	ASD TS	Updated to capture current capabilities and limitations
0.5	10/12/15	ASD TS	Complete draft including future capabilities that address current limitations
0.7		ASD TS	
1.0		ASD TS	

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	7/28/15	Jacqueline Meadows-Stokes	ITSM Enterprise Framework Design Pattern Lead
0.3	8/20/15	Jacqueline Meadows-Stokes	ITSM Enterprise Framework Design Pattern Lead
0.5	10/12/15	Jacqueline Meadows-Stokes	ITSM Enterprise Framework Design Pattern Lead
0.7		Jacqueline Meadows-Stokes	ITSM Enterprise Framework Design Pattern Lead
1.0		Jacqueline Meadows-Stokes	ITSM Enterprise Framework Design Pattern Lead

Draft

TABLE OF CONTENTS

CONTENTS

1 INTRODUCTION 1

1.1 Business Need 1
1.2 Approach 2

2 CURRENT CAPABILITIES AND LIMITATIONS 2

2.1 ITSM Frameworks and Standards in VA 2
2.2 Limitations 2

3 FUTURE CAPABILITIES 4

3.1 Alignment to Technical Reference Model (TRM) 8

4 USE CASES 9

4.1 Graphical Representation of DevOps 9
4.2 Graphical Representation of IT Governance Structure 10

APPENDIX A. DOCUMENT SCOPE 10

Scope 10
Intended Audience 11
Document Development and Maintenance 11

APPENDIX B. DEFINITIONS 13

APPENDIX C. ACRONYMS 16

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES 19

FIGURES

Figure 1: ITSM Current State 4
Figure 2: IT Management Frameworks & Standards 5
Figure 3: Proposed Enterprise ITSM Framework 6

TABLES

Table 1: Impact of Current Limitations 3
Table 2: Representative VA ITSM Enterprise Framework Categories and Approved Technologies 8
Table 3: Acronyms 16

Working Draft, Pre-Decisional, Deliberative Document - Internal VA Use Only

1 INTRODUCTION

Information Technology (IT) Service Management (ITSM) is the management of IT businesses and includes models for IT Planning, Support, Delivery, Security, and Infrastructure. ITSM Enterprise Framework provides the concepts and structures necessary to manage and govern IT resources and the lifecycle of services they deliver. The intent of IT frameworks are to establish guidance and best practices to control and improve the infrastructure, information, people, processes and investments (i.e., IT resources) required to deliver IT services. Frameworks like Federal Enterprise Architecture, Control Objectives for IT (CoBiT), and IT Infrastructure Library (ITIL) provide such guidance.

ITIL best practices are supplemented by a variety of standards, including the International Organization for Standardization (ISO) 20000-1 Service Management Standards and Capability Maturity Model Integration (CMMI). These standards provide the content, controls and activities required to successfully support adopting and integrating ITIL and ITSM. CMMI promotes the behaviors that lead to improved performance by defining what activities should be executed in relation to ITSM processes. ISO 20000-1 defines the work products and specific goals, which are used to assess ITSM processes efficiency and effectiveness.

The ITSM Enterprise framework establishes a common language, enabling consistency in planning, developing, delivering, and supporting IT services, and measuring IT resource performance. The consistency delivered by an enterprise framework is an important part of enabling agility in responding to business demand.

1.1 Business Need

Adopting an ITSM Enterprise framework in VA will provide a consistent and stable approach for developing, transitioning, operating and improving services. This process will transform VA's IT environment into a plug-and-play environment with the only variables being the technology (i.e., cloud, virtualization, mobile) used to deliver services and the knowledge needed to support the technology. Standardizing processes under the ITIL, framework, and ISO 20000-1 and CMMI for Services (CMMI-SVC) standards will:

- Improve interoperability across the enterprise
- Enable the move to a more homogeneous infrastructure
- Minimize security and cost risks through uniform domains
- Reduce cost through normalized configurations and assets
- Deliver consistent methods and practices to support the development and delivery of services

VA will have the capabilities to reduce operational complexity, identify and remove operational redundancies and inefficiencies, and focus on managing service delivery instead of managing infrastructure components.

Working Draft, Pre-Decisional, Deliberative Document - Internal Use Only

1.2 Approach

This design pattern describes a comprehensive ITSM framework that clearly defines enterprise-level IT management policies, standards, roles, responsibilities, and interfaces required to inform and guide IT programs.

The ITSM Enterprise Framework will be based on several frameworks and methodologies. The flexibility of this enterprise framework is the ability to adopt and use the best framework for specific processes and functions within the VA. Best practices and norms may come from bodies of knowledge such as the ITIL, CoBiT, the Capability Maturity Model (CMM), Six Sigma, the enhanced Telecom Operations Map (Business Process Framework), ISO/(International Electro Technical Commission) IEC 20000, ISO/IEC 27001, Total Quality Management, etc. Each has a particular area of emphasis but also brings consistency and ability to measure and improve performance. The ITSM Enterprise Framework will combine aspects of these frameworks, leverage existing best practices and provide a uniform and common language and is structured to provide guidance to improve effectiveness and efficiency.

The proposed approach enables cross-functional teams to create and improve processes in order to obtain the common goal of service excellence.

2 Current Capabilities and Limitations

2.1 ITSM Frameworks and Standards in VA

All VA regional data centers already have formal processes in place for customer contracts (service level agreements (SLAs), and operations and management (O&M) plans) to clearly define customer expectations. The Austin Information Technology Center (AITC) data center supports incident management via a certified professional on-site service desk that supports customers nationwide.

Regional data centers have a structured approach toward change management. Every change introduced into the environment requires a formal request for change that is reviewed by customer and/or data center change control boards (CCBs). Platform hosting services include: Infrastructure management (i.e., hardware, software, network, storage, database, etc.); Capacity management; Configuration management; Change management; Release management; Service level management; Availability management; Incident/Problem management; and Service desk management.

ProPath processes are in place to support full-lifecycle planning and execution of IT systems and services. All projects subject to PMAS are required to follow these processes in order to meet milestones and to deliver functionality to production environments.

2.2 Limitations

ITSM began as a set of disparate efforts to help guide, manage and improve IT service delivery and support. VA lacks an integrated framework that encompasses best practices from multiple frameworks, and provides guidance to establish the structure, documentation, and roles and responsibilities to plan, implement, monitor and improve ITSM.

Working Draft - Pre-Decisional, Deliberative Document - Internal VA Use Only

Table 1: Impact of Current Limitations

	Challenges	Impact
Limited Enterprise Level Alignment	- Program centric approaches to service delivery may not consider enterprise level IT strategies and initiatives - Current management capabilities, governance, processes, and tools are unique and not standard across the enterprise - Lack of common, enterprise level governance and decision making limits the ability to drive standardization and interoperability	- Gaps between enterprise level strategies and program specific goals - Limited enterprise visibility impacts efficiency of consolidation efforts
Unclear or undefined roles and responsibilities	- Acquisition responsibility at program level allows programs to create their own roles and responsibilities - Absence of a centralized IT SM Office and Sponsor	- Leads to disparate and disjointed IT management practices across the enterprise - Results in costs and program inefficiencies - Gaps in accountability of critical IT functions
Inadequate visibility into performance	- Individual programs do not have a common understanding of the operational impact of IT on the business	- Limits ability to identify inefficiencies and drive improvement of IT capabilities supporting VA's strategy and vision

The current state lacks a single data source view of information from various, distributed databases, and the ability to create management reports using intelligent information and trends. A variety of tools are disparately deployed:

- Asset management - (AEMS/MERS, Maximo, SCCM, CA-Unicenter, BMC, and others)
- Configuration Management - (SCCM, CA-Unicenter, BMC, Serena and others)
- Financials Management - (IFCAP, FMS, FLITE, Maximo and others),
- Systems and Performance Management - (collected data from network, server, and desktop management tools)
- Security Data - (SCCM, STAT Guardian, Patchlink and others that collect provide information security compliance data)
- Help Desk information including Incident, Problem and Customer Management (BMC Remedy and ESS, CA, Serena and others).

Working Draft, Pre-Decisional Deliberative Document - Internal VA Use Only

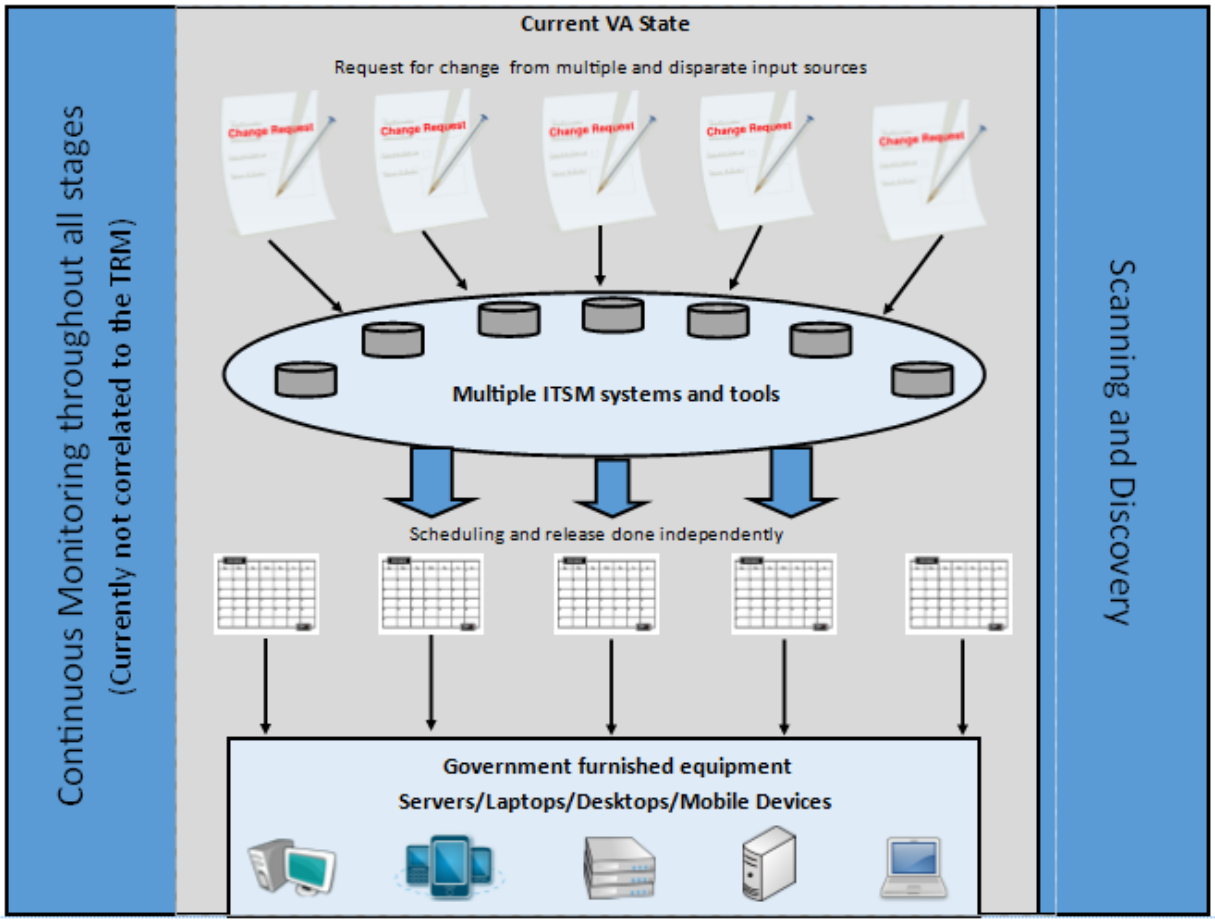


Figure 1: ITSM Current State

Working Draft, Pre-Decisional Do

3 FUTURE CAPABILITIES

VA Service management must address unique requirements of a multi-vendor environment and ensure situational awareness. The VA Enterprise Framework provides the structure under which standards, specifications and procedures for enterprise ITSM is built. The ITSM enterprise framework provides the structure under which standards, specifications and procedures for enterprise IT service management is built.

Guiding principles and constraints for establishing the framework consistently for future IT services is as follows:

Enterprise ITSM Framework

Establish an enterprise wide ITSM Framework leveraging industry standards and maturity models.

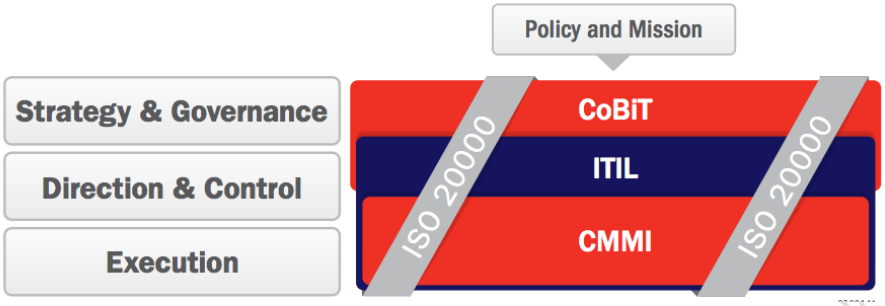


Figure 2: IT Management Frameworks & Standards

Industry recognized ITSM frameworks and maturity models will help improve service management functions and processes, and implement best practices (see Figure 2).

An integrated enterprise framework facilitates operational effectiveness, ensure continuous improvement, reduce defects, and provide better visibility	
ISO	Provides a set of requirements for an integrated process approach to deliver managed services. ITIL can be leveraged to develop ISO 20000 compliant processes.
CoBiT	Provides a business framework for the governance and management of Enterprise IT.
ITIL	Plan, manage and continually improve services to ensure they are meeting business goals and delivering value.
CMMI	Ensure consistency in service delivery, process improvement that delivers cost savings. CMMI helps improve the capability to consistently and predictably deliver products and services to customers when they want them and at a cost effective price.

Working Draft, Pre-Decisional, Deliberative Document - Internal VA Use Only

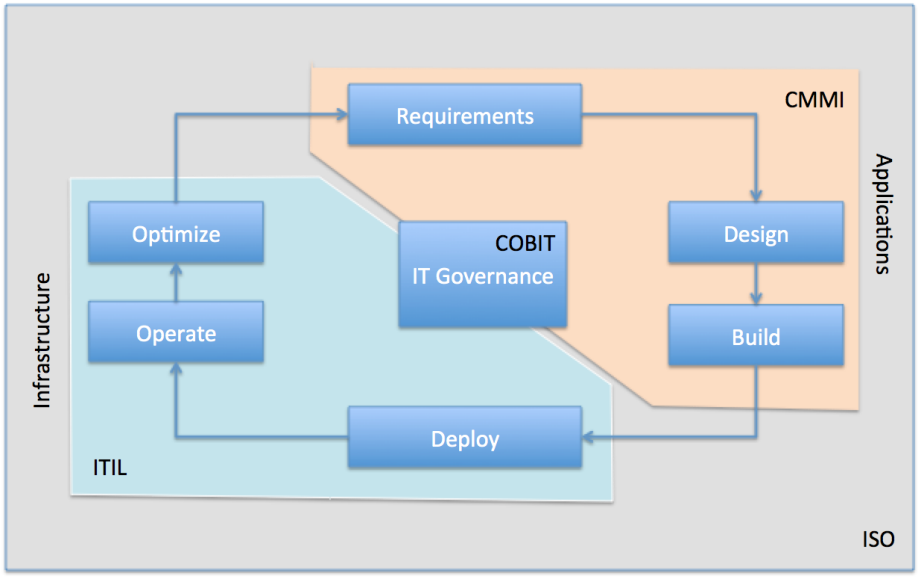


Figure 3: Proposed Enterprise ITSM Framework

An effective Enterprise ITSM Framework includes well-defined and documented processes that demonstrate superior IT services delivery. The processes are integrated and operate at a measurable and standardized maturity level. The customer expectations are documented and process improvement activities are based on a combination of customer expectations and the process maturity results.

ITSM Policy and Standards Compliance

Integrate compliance mechanisms into existing enterprise level governance processes establishing accountability, enforcing service management standards and driving interoperability and consistency across IT acquisitions.

Policies and standards of an enterprise governance structure, enabled with necessary compliance mechanisms and controls, need to be established to effectively promote adoption of enterprise-level ITSM frameworks. This structure should serve to monitor, manage and report command and program level adherence. By using the VA Enterprise Architecture (EA), VA can prescribe ITSM policies enforcing Enterprise Technical Architecture (ETA) compliance and standards. All VA IT systems are required to comply with the EA. In addition to demonstrating compliance through business cases, IT acquisition programs should conduct frequent, iterative technical reviews to ensure interoperability with the enterprise ITSM framework.

Working Draft, Pre-Decisional, Deliberative Document - For Internal Use Only

Clearly Defined Roles and Responsibilities

Identify, define and promulgate enterprise level roles and responsibilities.

Roles and responsibilities with individual programs may exist and can be well defined but are not often aligned to enterprise wide requirements. To successfully drive awareness and adoption of enterprise ITSM standards, it is critical that the enabling roles and responsibilities are clearly defined and accepted across all lines of business. This means that the programs that make up IT management must not only have the authority to fulfill responsibilities but also have a firm understanding on the impact. Clear demonstration of the relationships among IT management responsibilities, the services delivered and the supported mission is foundational to that understanding.

IT Service Rationalization

Rationalize existing IT services and service management capabilities against enterprise ITSM framework.

All existing IT assets should directly support or contribute to customer-facing IT services. With an Enterprise ITSM Framework, the relationships between those elements should be described, documented and well understood. Existing IT infrastructure and services should be continually assessed and rationalized against that architecture and the business need to identify and maintain those relationships in the current operating environment.

Enterprise IT Service Management Office

Establish an enterprise-level ITSM office to inform IT acquisitions, oversee, and align program level ITSM initiatives across VA in support of enterprise efficiency and consolidation efforts.

With VA, traditional service management functions are distributed or fragmented across the lines of business, programs and locations often with differing, and in some cases competing, priorities. The establishment of a centralized, enterprise-level ITSM office ensures standardization and integration across disparate initiatives.

The Office should align to the IT Leadership Board (ITLB) and the Enterprise Architecture Council (EAC), and be given authority to oversee and report on all ITSM matters. Existing program ITSM initiatives, projects and any working groups should be aligned to this office. Responsibilities should include:

- **ITSM Strategy and Governance**: Establish ITSM Strategy, vision, and supporting governance structure for VA
- **Strategic Communications**: Manage communications with key stakeholders and governance boards

Working Draft, Pre-Decisional, Deliberative Document - Internal VA Use Only

- **Standards Compliance**: Develop Enterprise ITSM Framework aligned with the TRM, define standards and conventions, develop compliance measures, and monitor and report compliance
- **Quality Management**: Establish enterprise wide quality management program
- **Architecture & Integration**: Facilitate integration and prioritization of ITSM initiatives
- **Training**: Develop ITSM training and awareness program
- **Process Improvement**: Oversee and support execution of process improvement efforts in compliance with process and quality standards
- **Acquisition Support**: Support the reform of acquisition processes and practices to ensure ITSM framework and principles are incorporated

Training and Outreach Program

VA will use a training and outreach program to deliver technical product training and certification preparation and exercises. A Training and outreach program will provide VA employees common language and internal skills necessary for stakeholders to be on the same page. Training aligns organizational changes with efforts to support behavior change and will cover topics such as:

- Designing IT Service Management Vision and Strategy
- Implementing Roadmap Training
- Managing Organizational Change
- Developing Processes

Training Goals and Objectives:

- Creating a level of understanding and awareness about IT Service Management and ITSM programs
- Using key internal resources or consultants to become internal experts
- Increasing ITIL knowledge
- Identifying new skills and competence levels required to support processes
- Using training to communicate ITSM program information

3.1 Alignment to Technical Reference Model (TRM)

The VA Technical Reference Model (TRM) is a component within the overall EA that establishes a common vocabulary and structure for describing the IT used to develop, operate, and maintain enterprise applications.

All projects are required to use the approved tools and technologies located in the TRM in order to comply with the architectural guidance provided in this document. Table 1 includes relevant tools.

Table 2: Representative VA ITSM Enterprise Framework Categories and Approved Technologies

Tool Category	Example Approved Technologies
Configuration Management Database (CMDB)	**CA Service Desk Manager, BMC Remedy, Legacy CMDBs**
Endpoint Manager	**IBM Endpoint, Microsoft SCCM**

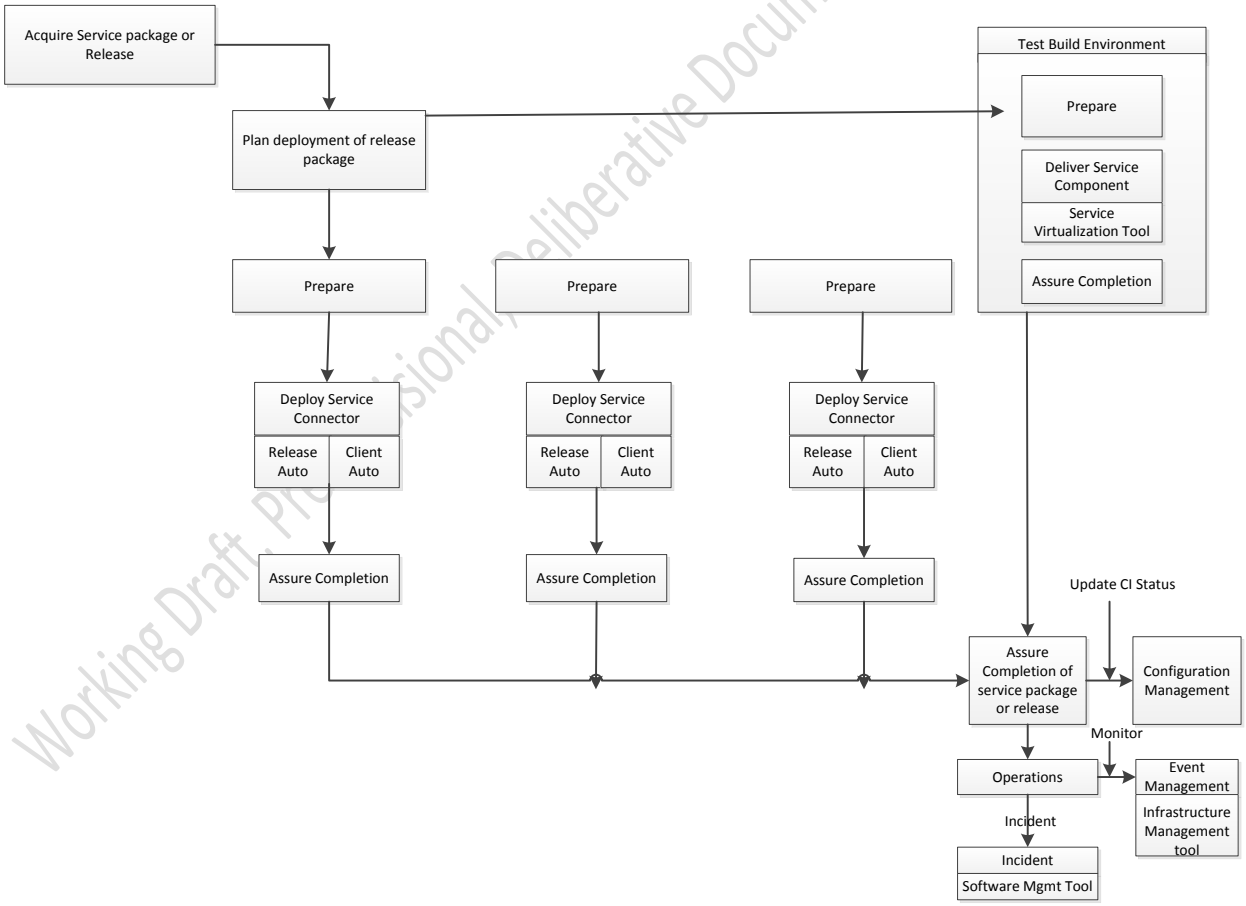
Working Draft, Pre-Decisional, Deliberative Document - Internal VA Use Only

Patch Management	**IBM Endpoint, Microsoft SCCM**
Asset Management	**CA IT Asset Manager**
Relationship and Dependency Mapping	**BMC ADDM, CA Configuration Automation**
Line of Business	**VA System Inventory**
Configuration Change Control	**CA Configuration Automation**
Data Normalization	**BMC ADDM, CA IT Asset Manager (SAM component.**
Scanning and Discovery	**Nessus, IBM Endpoint, Microsoft SCCM, CA Configuration Automation**

4 USE CASES

4.1 Graphical Representation of DevOps

The diagram represents the process inputs, outputs and triggers along with visual interaction between multiple capabilities, and tools showing process task automation.

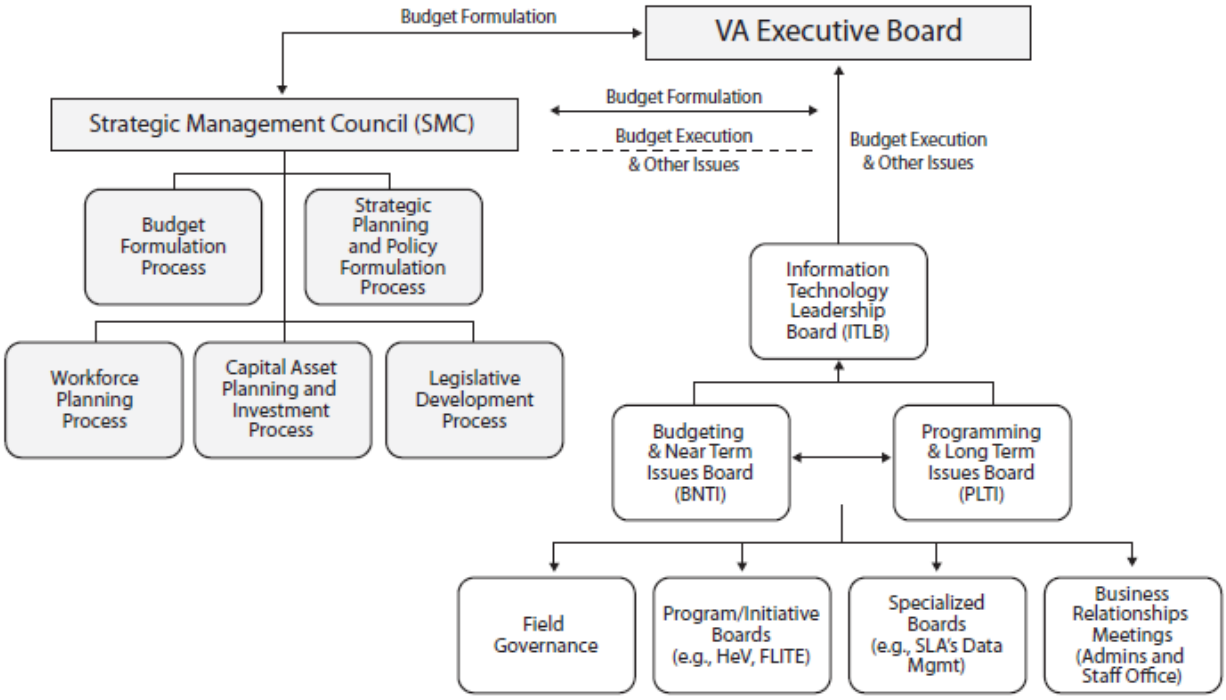


Working Draft, Provisional, Deliberative Document - Internal VA Use Only

4.2 Graphical Representation of IT Governance Structure

The IT Governance structure is developed based off of Industry best practices including COBIT and ITIL and other standards to provide a framework for IT governance structure and plan. This structure creates a system that meets VA's IT needs to build and maintain key applications, support operations, and monitor IT in five key areas:

- Enterprise management
- Business management
- Business application management
- Infrastructure
- Service support



Appendix A. Document Scope

Scope

The ITSM Enterprise Framework Design Pattern provides vendor-agnostic guidelines for establishing a framework for standardized ITSM processes and tools at VA. Implementation of common processes and tools will standardize ITSM activities to ensure a consistent approach to managing VA's IT infrastructure in accordance with VA and Federal security policies. Applying a standard ITSM framework supports cross-organizational change management, risk management, and quality, enabling SDE Enterprise Operations to manage services and supporting infrastructures in a controlled manner.

Intended Audience

This document is intended for use by all project-level integrated product teams (IPTs) which includes the following:

- All IPTs that develop or acquire IT systems subject to the Project Management Accountability System (PMAS) will refer to Enterprise Design Patterns
- The OneVA Enterprise Technical Architecture (ETA) Compliance Criteria refers to approved Enterprise Design Patterns as an authoritative source for guiding and constraining solution design
- IPTs will be evaluated for use of enterprise capabilities described in the Enterprise Design Patterns during PMAS Milestone Reviews
- System Design Documents (SDD) are reviewed for compliance in Architecture and Engineering Review Board (AERB) reviews

Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from OI&T, PD, OIS, ASD, and SDE. Extensive input and participation was also received from VHA, VBA and NCA. Development of the document included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

An Enterprise Design Pattern is a capability guidance document that identifies best practice approaches to solving reoccurring technical problems. It enables the reuse of enterprise capabilities in standard ways.

- Enterprise Design Patterns are:
  - Limited enough to be usable and broad enough to be reusable
  - Formalized, validated best practices that projects will leverage in the establishment of their solution architecture
  - Guide stakeholders to implementation resources that they will use to establish design specifications for system development and integration
- Enterprise Design Patterns are NOT:
  - Project-specific solution architectures
  - Implementation policy or directives
  - Software development kits
  - Set of approved tools and technologies (this is covered by the TRM)

In addition, the Technology Strategies team engages industry, external government agencies, and academic experts through Vendor Engagements and Public Forums to review, provide input, and comment on proposed patterns.

Working Draft, Pre-Decisional, Deliberative Document - Internal VA Use Only

Approved versions of Enterprise Design Patterns can be found at the Tech Strategies Website: http://www.techstrategies.oit.va.gov/docs_design_patterns.asp)

Updates to approved design patterns will be coordinated with the Office of Technology Strategies' lead, who will facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

In July 2014, Deputy Chief Information Officer (DCIO) ASD formally signed and approved the first increment of the IT Service Management (ITSM) Enterprise Design Pattern. This increment is the Configuration Management Enterprise Design Pattern and TS will continue to develop future increments.

Working Draft, Pre-Decisional, Deliberative Document - Internal VA Use Only

Appendix B. Definitions

Name	Definition
Capability Maturity Model Integration (CMMI)	Process improvement training and appraisal program and service administered and marketed by Carnegie Mellon University and required by many DOD and U.S. Government contracts, especially in software development.
Change Control Board (CCB)	Committee that makes decisions regarding whether or not proposed changes should be implemented. Agreed upon changes are communicated to the project team and client and the requirement is baselined with the change.
Change Management	Standardized methods and procedures used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service.
Cloud Computing	Internet-based computing, where shared resources and information are provided to computes and other devices on-demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources
Configuration	The possible conditions, parameters, and specifications with which an information system or system component can be described of arranged.
Configuration Change Control	Process for managing updates to the baseline configurations for the configuration items; and evaluation of all change requests and change proposals and their subsequent approval
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development and production life cycle.
Configuration Monitoring	Process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under CM.
Control Objectives for IT (CoBiT),	Framework created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control

Working Draft, Pre-Decisional, Deliberative Document - Internal Use Only

Name	Definition
	requirements, technical issues and business risks.
Enterprise Architecture	The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.
Federal Enterprise Architecture	The enterprise architecture of a federal government. It provides a common approach for the integration of strategic, business and technology management as part of organization design and performance improvement
Information Technology Infrastructure Library (ITIL)	Set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. ITIL describes processes, procedures, tasks, and checklists which are not organization specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It is used to demonstrate compliance and to measure improvement
International Electrotechnical Commission (IEC)	Non-profit, non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic, and related technologies.
International Standards Organization (ISO) 20000-1	Includes the design, transition, delivery, and improvement of services that fulfill service requirements and provide value for both the customer and the service provider.
Patch	An additional piece of code developed to address a problem in an existing piece of software.
Program Management Accountability System	Ensures that the customer, IT project team, vendors, and all stakeholders engaged in a project are focused on a single, compelling mission to achieve on-time project delivery.
ProPath	Established in order to enhance and encourage a standard comprehensive process framework across the organization.
Risk Management	Identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of

Working Draft, Pre-Decisional Deliberative Document - Internal Use Only

Name	Definition
	opportunities.
Service Level Agreement (SLA)	Part of a standardized service contract where a service is formally defined. Particular aspects of the service – scope, quality, responsibilities – are agreed between the service provider and the service user.
Six Sigma	A disciplined, data-driven approach and methodology for eliminating defects in any process – from manufacturing to transactional and from product to service.
Telecom Operations Map	A model that describes the required business process of service providers, and defines key elements and how they should interact.
Total Quality Management (TQM)	Comprehensive and structured approach to organizational management that seeks to improve the quality of products and services through ongoing refinements in response to continuous feedback.
Virtualization	The act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, operating systems, storage devices, and computer network resources.

Working Draft, Pre-Decisional, Deliberative Document - Internal VA Use Only

Appendix C. Acronyms

The following **Error! Reference source not found.**provides a list of acronyms that are applicable to and used within this Enterprise Design Pattern document.

Table 3: Acronyms

Acronym	Description
ADDM	Atrium Discovery and Dependency Mapping
AITC	Austin Information Technology Center
ASD	Architecture, Strategy and Design
CA	CA Technologies
CA SDM	CA Service Desk Manager
CCB	Change Control Board
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
CMMI	Capability Maturity Model Integration
CoBiT	Control Objectives for IT
COTS	Commercial Off-the-shelf
EAC	Enterprise Architecture Council
EO	Enterprise Operations
ESE	Enterprise Systems Engineering
ETA	Enterprise Technical Architecture
FEA	Federal Enterprise Architecture
GOTS	Government Off-the-shelf

Draft

Acronym	Description
IBM EPM	IBM Endpoint Manager
IEC	International Electrotechnical Commission
IS	Information System
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITLB	Information Technology Leadership Board
ITSM	Information Technology Service Management
NIST	National Institute of Standards and Technology
NSD	National Service Desk
OI&T	Office of Information and Technology
OIG	Office of the Inspector General
OIS	Office of Information Security
O&M	Operation and Management
OMG	Office of Management and Budget
OVAL	Open Vulnerability Assessment Language
PD	Product Development
PMAS	Program Management Accountability System
SCCM	System Center Configuration Manager
SDE	Service Delivery Engineering
SLA	Service Level Agreement
TRM	Technical Reference Model

Draft

Acronym	Description
TQM	Total Quality Management
VA	Department of Veterans Affairs
VASI	Veterans Affairs Systems Inventory

Draft

Appendix D. References, Standards, and Policies

This Enterprise Design Pattern is aligned to the following VA OI&T references and standards applicable to all new applications being developed in VA, and are aligned to VA ETA:

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA Directive 6004	Directive establishes VA policy and responsibilities regarding Configuration, Change, and Release Management Programs for implementation across VA.
2	VA	VA 6500 Handbook	Directive information security program. Defining overall security framework for VA.
3	NIST	800-128	Guide for Security-Focused Configuration Management of Information Systems Provides guidelines for organizations responsible for managing and administrating the security of federal information systems and associated environments of operations
4	NIST	SP 800-63-2	Special Publication — Creating a Patch and Vulnerability Management Program Designed to assist organizations in implementing security patch and vulnerability remediation programs.
5	NIST	800-53	Recommended Security Controls for Federal Information Systems and Organizations Outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks
6	OMB	Memorandum M-14-04	FY2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management Provides guidance for Federal agencies to follow the report requirements under FISMA.
7	OMB	Memorandum M-02-01	Guidance for Preparing and Submitting Security Plans of Actions and Milestones Defines Management and Reporting Requirements for agency POA&Ms, including deficiency descriptions, remediation actions, required resources, and responsible parties.

Draft

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
8	White House	FISMA Act of 2002	Reauthorizes key sections of the Government Information Security Reform Act Provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets.
9	VA	CRISP	Intended to improve access controls, configurations management, contingency planning, and the security management of a large number of information technology systems.
10	Congress	E-Government Act of 2002	Public Law 107-347 Purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes.
11	VA	Change Plan – Process Template	This Standard Operating Procedure has been created to support and supplement the National Change Management Policy and Standard Document and is not intended to replace the overall management process of the Change Management Program this SOP expands and provides specific information related to the following process being placed under Change Control
12	VA	OIT Enterprise Change Management Policy	This document establishes an OIT Enterprise Change Management policy ensuring changes to all information technology infrastructure and software configuration items (CIs) are managed and communicated in a disciplined and standardized manner to minimize risk, impact and optimize IT resources
13	VA	OIT Change Management Process	The purpose of the Change Management (ChM) process is to provide guidance for the management of changes to all Department of

Draft

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
			Veterans Affairs (VA) Information Technology (IT) environments. The process provided guidance on how to manage a change throughout its life cycle.

Draft