
VA Enterprise Design Patterns: IT Service Management (ITSM)

Disaster Recovery Planning

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

Version 1.0

Date Issued: October 2016



THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

Gary Marshall
Director, Technology Strategies, ASD

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

REVISION HISTORY

Version	Date	Organization	Notes
0.1	7/11/16	ASD TS	Initial Draft/Outline
0.3	8/10/16	ASD TS	Second draft document with updates made throughout document based upon initial internal/external stakeholder review and comment.
0.5	9/19/16	ASD TS	Updated draft for community review prior to TS leadership approval/signature. Updates made following Public Forum collaborative feedback and working session.
0.7	9/25/2016	ASD TS	Updates made following Public Forum collaborative feedback and working session.
1.0	10/19/2016	ASD TS	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance.

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	7/22/2016	Jacqueline Meadows-Stokes	Enterprise Design Pattern Lead
0.3	8/9/2016	Jacqueline Meadows-Stokes	Enterprise Design Pattern Lead
0.5	9/20/2016	Jacqueline Meadows-Stokes	Enterprise Design Pattern Lead
0.7	10/18/2016	Jacqueline Meadows-Stokes	Enterprise Design Pattern Lead

TABLE OF CONTENTS

1	INTRODUCTION	3
1.1	BUSINESS PROBLEM.....	3
1.2	BUSINESS NEED	5
1.3	BUSINESS CASE.....	5
1.4	APPROACH.....	5
2	CURRENT CAPABILITIES	6
2.1	CURRENT CAPABILITY AND LIMITATIONS	7
2.1.1	<i>ENTERPRISE ROLE</i>	<i>7</i>
2.1.2	<i>DRP DEVELOPMENT PROCESS.....</i>	<i>8</i>
3	FUTURE CAPABILITIES.....	9
3.1	ENTERPRISE TECHNICAL GOVERNANCE	9
3.1.1	<i>Objective and Impact.....</i>	<i>9</i>
3.1.2	<i>Approach.....</i>	<i>9</i>
3.2	AVAILABILITY OF AUTOMATION.....	13
3.2.1	<i>Objective and Impact.....</i>	<i>13</i>
3.2.2	<i>Approach.....</i>	<i>13</i>
3.3	ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM)	15
3.4	ALIGNMENT TO VETERAN-CENTRIC INTEGRATION PROCESS (VIP).....	15
4	USE CASES	16
4.1	USE CASE 1 – APPLYING VA ENTERPRISE TGT OVERSIGHT	16
4.1.1	<i>Purpose</i>	<i>16</i>
4.1.2	<i>Assumptions.....</i>	<i>16</i>
4.1.3	<i>Use Case Description.....</i>	<i>17</i>
4.2	USE CASE 2 – WORKFLOW AUTOMATION SUPPORT FOR DRPs.....	18
4.2.1	<i>Purpose</i>	<i>18</i>
4.2.2	<i>Assumptions.....</i>	<i>18</i>
4.2.3	<i>Use Case Description.....</i>	<i>18</i>
	APPENDIX A: SCOPE	21
	APPENDIX B: DEFINITIONS	23
	APPENDIX C: ACRONYMS	26
	APPENDIX D: REFERENCES, STANDARDS, AND POLICIES	28
	APPENDIX E: VA DRP POLICIES AND DIRECTIVES	29
	APPENDIX F: ISCPA PROCESS	30

FIGURES

Figure 1. DRP Development and Management Process at VA 6

TABLES

Table 1: VA Resources for DRP Development..... 13
Table 2: Representative VA ITSM Enterprise Framework Categories and Approved Technologies..... 15

1 INTRODUCTION

In 2013, Hurricane Sandy affected 24 states, killed 233 people, and caused nearly \$75 Billion worth of damage. A Department of Veterans Affairs (VA) medical facility, VA New York Harbor Healthcare System-Manhattan, experienced significant damage which led to catastrophic failure of all the major utility systems that service the building¹. As a result, patients were evacuated and critical processes and systems were redirected to nearby facilities. The facility remained closed for 6 months while updates to the infrastructure, processes, and information technology (IT) systems occurred. The damage resulted in a \$207 million Federal investment to both update emergency procedures and increase the readiness posture, infrastructure, and IT systems during a disaster or emergency.

The events at VA New York Harbor Healthcare System-Manhattan during Hurricane Sandy underscore VA's need to have procedures in place to adequately plan for, respond to, and recover from disasters or emergencies. The restoration of IT systems after an emergency is imperative to VA's mission.

Disaster recovery planning guides the immediate recovery of critical IT systems to normal operations in the event of a disaster or extended critical disruption at a VA facility. A Disaster Recovery Plan (DRP) refers to an IT-focused plan that²:

- Activates due to major system disruptions.
- Restores operability of one or more information systems at an alternate site, utilizing the contingency plans of several individual IT systems.
- Details the relocation of information systems operations to an alternate location.

DRP templates at VA comply with all applicable Federal and current VA Policies and Directives. These policies are listed in Appendix E.

1.1 BUSINESS PROBLEM

In Fiscal Year (FY) 2015, VA Office of Inspector General (OIG) conducted an audit to assess the compliance of VA's information security program against Federal Information Security Modernization Act (FISMA) requirements and applicable National Institute of Standards and Technology (NIST) guidelines. NIST standards and guidelines are mandatory and binding for federal agencies by the Secretary of Commerce under statutory authority. FISMA provides a

¹ VA.GOV VA NY Harbor Healthcare System Press Release

² NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. OIG audit teams assessed VA's information security program through inquiries, observations, and tests of selected controls supporting 55 major applications and general support systems at 26 VA facilities. The teams identified specific deficiencies in 8 areas including disaster recovery. The assessment of the information security program uncovered DRPs that were³:

- Outdated in that some Information System Contingency Plans (ISCPs) had not been updated to reflect detailed disaster recovery procedures for all system components or reflect current operating conditions. ISCPs and DRPs address IT systems having a high critical exposure ranking. Accurate ISCP data is essential to the development of a viable DRP.
- Incomplete in that they did not clearly identify alternate processing and storage sites.
- Inadequate in that they did not always document backup and detailed recovery procedures used to restore systems.

The OIG audit report also contained:

- Recommendations for improving the information security program.
- Status of prior recommendations and corrective action plans.
- List of successfully closed recommendations in FY 2015.

The current DRP development and management process at VA contributes to defects that may impede timely restoration of systems in the event of system disruption or disaster. OIG audit findings are consistent with key defects identified by disaster recovery planning teams across VA including the lack of governance, quality control, and automation.

Several VA organizations involved in disaster recovery planning have noted the following at both the enterprise and regional levels:

- Compliance with the disaster recovery planning process is not consistent across the enterprise.
 - No organization within VA has the authority to enforce DRP completion.

³ Department of Veterans Affairs Federal Information Security Modernization Act Audit for Fiscal Year 2015

- The approved template provided by the Office of Business Continuity (OBC), which guides the development and implementation of emergency management and continuity plans for VA organizations, is not always used.
- Annual updates to DRPs are not consistently completed.
- The quality level of information captured in DRPs depends on the knowledge level of the personnel completing the DRP. When these personnel do not have a complete understanding of onsite IT systems, it impacts the resulting DRP.
 - This creates the risk that DRPs are not executable when needed.
- DRP development and maintenance involves a manual process that contributes to inconsistencies in data entry and plan completeness.

1.2 BUSINESS NEED

The Disaster Recovery Planning Enterprise Design Pattern (EDP) provides a framework for establishing efficient and effective restoration of systems in the event of system disruption or disaster. Capabilities identified in this EDP will support enhanced enterprise disaster recovery planning that is accurate, reflects current IT systems onsite, and incorporates updates that are congruent with current IT systems, DRP testing results, and action items. The EDP will identify best practices for bridging VA disaster recovery planning gaps identified in Section 1.1.

1.3 BUSINESS CASE

The Disaster Recovery Planning EDP guidance to VA stakeholders bridges enterprise-wide DRP gaps and ensures that IT systems, data, and assets are able to return to normal operations after a major disruption or emergency. Disruptions or emergencies include localized acts of nature, accidents and attack-related events. This document provides guidance to VA organizations involved in planning, responding to, and recovering VA IT systems. This verifies compliance with all directives and policies in Appendix D, including NIST 800-34, Rev 1 and VA Handbook 6500.8.

1.4 APPROACH

The EDP will look at current capabilities for disaster recovery planning within VA to address:

- Governance structure for overseeing disaster recovery planning throughout the enterprise.
- Best practices for DRPs that are accurate, complete, and viable.
- Leveraging an enterprise-level disaster recovery planning lifecycle process tool to foster collaboration and transparency.

2 CURRENT CAPABILITIES

VA has in place a disaster recovery planning process, shown in Figure 1. A DRP captures the restoration requirements and activities to employ in the case of a major IT system disruption or disaster to restore affected capabilities.

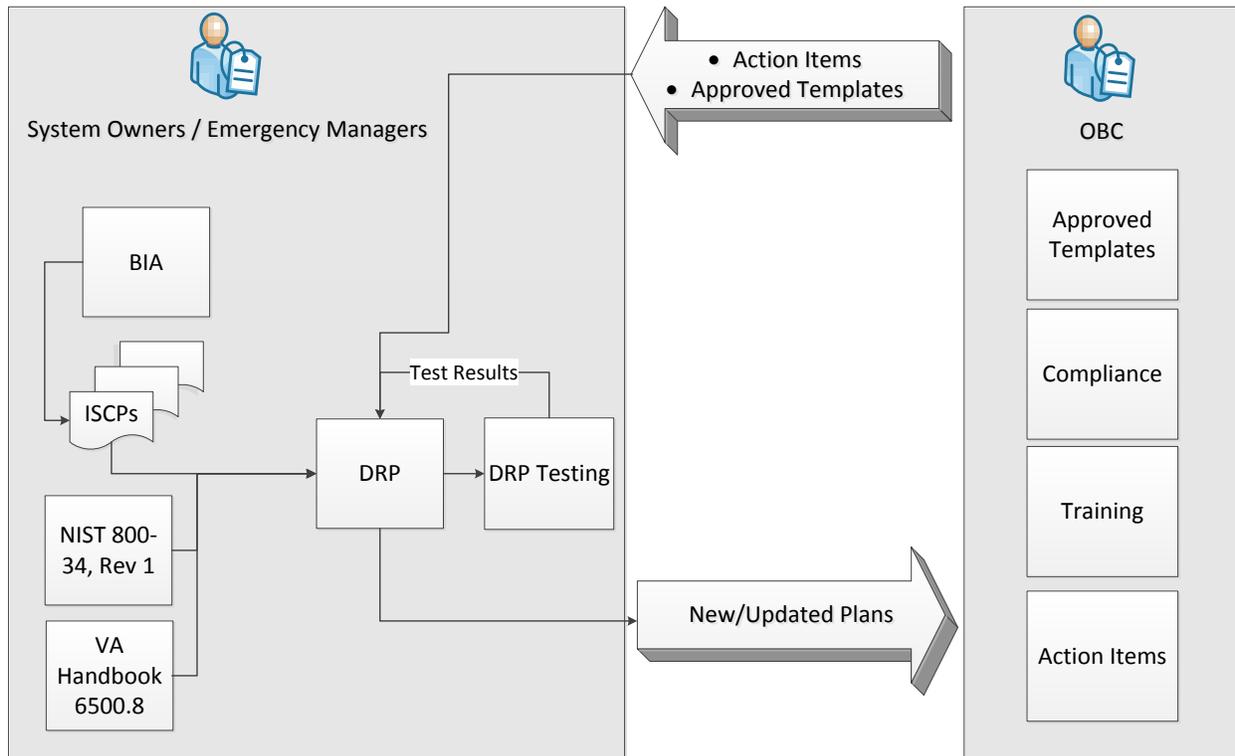


Figure 1. DRP Development and Management Process at VA

OBC provides Emergency Management Teams (EMTs), consisting of Emergency Managers (EMs) and System Owners (also referred to as Subject Matter Experts [SMEs]) with approved DRP templates and action items. The information submitted in the templates does not consistently satisfy and meet OIG approval standards.

EMTs are responsible for developing, testing, and updating the DRPs for VA Enterprise Information Technology Centers (ITCs), Regional Data Centers, and Medical Centers. EMTs leverage information from relevant system Business Impact Analysis (BIA) and ISCP documents along with guidance and policies outlined in NIST 800-34 and VA Handbook 6500.8 to develop a DRP for their respective facilities.

After the DRP is written, SMEs conduct testing, including table top exercises and training for operation staff on the procedures outlined in the DRP. Test results drive updates to the DRP. Once the SMEs have written and tested the plans, OBC reviews and approves. OBC review

consists of checking that required fields are populated, but not necessarily that they are correct.

OBC also trains teams on how to populate the template and coordinates assistance with EMTs.

2.1 CURRENT CAPABILITY AND LIMITATIONS

Stakeholders cited key aspects of the current DRP development and management process for improvement to enhance disaster recovery planning across the enterprise. Discrepancies have been identified in:

- Disaster recovery planning enterprise roles.
- The process to develop and maintain DRPs.

2.1.1 ENTERPRISE ROLE

OBC oversees the disaster recovery planning process within VA. Per VA Handbook 6500.8, the OBC has been tasked with “developing and maintaining the IS Contingency Planning Assessment (ISCPA) process and associated ISCP and DRP templates and standards for their completion.” OBC updates these DRP templates annually and disseminates them to EMTs along with action items to be addressed. OBC reviews submitted DRPs for completeness in accordance with NIST 800-34 Rev1 and VA Handbook 6500.8.

OBC works with EMs to ensure that SMEs are properly trained and informed of the ISCPA process as described in VA Handbook 6500.8. A DRP can become non-compliant due to insufficient documentation. OBC offers SMEs the opportunity to submit a Risk Based Decision (RBD) in order to document issues contributing to non-compliance. Examples of non-compliance include incomplete documentation of recovery procedures and system components. SMEs provide a mitigation strategy for the RBD to the Office of Cyber Security (OCS) including a path forward for reaching a solution. The mitigation strategy must be approved by the Information Security Officer (ISO) in order to obtain or maintain the Authority to Operate (ATO).

OBC provides guidance to EMTs in the DRP development process; however they lack the authority to regulate DRP completion, maintenance, and content. If an incomplete DRP is submitted or an update is not performed, OBC can reject the submission or note that the action item was not completed, but cannot enforce further action. Incomplete or outdated DRPs increase the risk that critical VA systems cannot be restored in the event of an emergency.

2.1.2 DRP DEVELOPMENT PROCESS

At the start of each fiscal year OBC updates the DRP template. Updates to the DRP are then disseminated as action items to teams in the field. Auditable DRPs begin with completing the five-step ISCPA Process as illustrated in Appendix F. Each step of the process requires collaboration between the author and specific role-based facility personnel with intimate knowledge of the facility systems. After completing the first four steps, the author identifies and prioritizes the exposures and risks for general support systems and critical applications, which must be accounted for in the site DRP. The finalized DRP is housed in a SharePoint portal and is used to track whether or not plans are completed.

VA previously used an Information System Contingency Planning Assessment (ISCPA) tool that provided multiple benefits for DRP development. Some of the benefits included:

- Data mining capabilities.
- Granularity in the reporting process between phases of plan completion.
- An easy and effective review and approval process.
- Consistently managed changes in the template and the information requested therein.
- Information as to where in the development process an organization is in completing the DRP.

However, VA Service Delivery and Engineering (SDE) Enterprise Operations (EO) is the only organization currently using an automation tool to develop DRPs. The SDE EO tool tracks DRP development and provides plan updates to personnel responsible for disaster recovery planning. The remainder of the enterprise uses a manual DRP process which contributes to the following limitations:

- Plan Authors manually replicate changes across multiple plans, as there is no method to manage global editing/updates across the enterprise.
- Changes made to plans by Plan Authors are not tracked, resulting in time-consuming reviews by OBC.
- Plan Authors are required to identify the name and contact information of responsible personnel for each IT System. Although VA's Global Address List (GAL) is used as an authoritative source for this information, transferring it from the GAL to the template potentially allows the possibility of human error.
- The template does not have flexibility to account for emerging technology (e.g. cloud storage).

While the OBC developed DRP template is compliant with Federal and current VA policies, the information contained within the DRP template does not comply with OIG approval standards. Outdated policy guidance from VA Handbook 6500.8 references the Security Management and Reporting Tool (SMART) when VA actually uses RiskVision Governance Risk and Compliance (GRC) as a repository for DRPs. The fields within the template are out of date and do not reflect:

- Migrations of systems from individual medical facilities to a Regional Data Center.
- Modern technology like cloud storage eliminates the need for an alternate processing site.

3 FUTURE CAPABILITIES

3.1 ENTERPRISE TECHNICAL GOVERNANCE

3.1.1 Objective and Impact

Standardizing disaster recovery planning guidance fixes the lack of enforcement/accountability which results in compliance inconsistencies and the subsequent risk of non-viable plans. A VA Enterprise Technical Governance Team (TGT) would:

- Provide standardized disaster recovery planning guidance throughout the DRP development and maintenance lifecycle.
- Ensure accountability and enforcement compliance with DRP policies.

In standardizing disaster recovery planning guidance, the TGT will enhance compliance and viability. Compliance is achieved when defined roles and uniform checklist of processes are utilized by all responsible for DRP development. Viability is promoted through the use of a standard framework to follow which minimizes ambiguity in DRP development.

3.1.2 Approach

The TGT for disaster recovery planning will:

- Identify the standard core guidelines and workflow for Plan Reviewers and Plan Authors.
- Identify and recommend appropriate training.
- Identify and recommend tests and exercises.
- Identify enterprise criteria for baseline DRPs.
- Apply lessons learned.

A representative sample of personnel with intimate domain knowledge for developing and maintaining DRPs will compose the TGT. TGT members should include SMEs, EMs, ISOs, and Emergency Planner (EP) Division Chiefs.

3.1.2.1 Identify Standard Core Guidelines and Workflow for Plan Reviewers and Plan Authors

The TGT identifies core guidelines and workflows for Plan Reviewers and Plan Authors. The guidelines will trace to VA Handbook 6500.8 and be consistent with policy updates. The Disaster Recovery Planning EDP will be updated to reflect changes to VA Handbook 6500.8 and other relevant policies.

Facility-level Plan Reviewers (ISOs) ensures that the DRP is vetted through third party technical experts with DRP domain knowledge. Plan Reviewers at the regional level (EP Division Chiefs, EMs) review the DRP before it is submitted to Plan Reviewers at the enterprise-level (OBC). Plan Reviewers at the regional level coordinate with Plan Reviewers at the facility level or onsite personnel with more intimate knowledge of the systems.

Plan Authors (SMEs, Systems Owners) need to know where to obtain the DRP template and document that they coordinated with Plan Reviewers at the enterprise-level to begin the DRP development process.

3.1.2.2 Identify and Recommend Appropriate Training

The TGT identifies and recommends disaster recovery training for Plan Authors and Plan Reviewers. The training will

- Increase understanding of the purpose of the DRP.
- Demonstrate how to properly develop a DRP.
- Establish the roles and responsibilities of all personnel involved in DRP development.

A virtual training delivery strategy will be the most efficient and practical approach.

Plan Authors and Plan Reviewers require DRP development training, which includes:

- Familiarity with the Business Continuity (BC) portal and its key resources.
- Understanding of the DRP template and its requirements.
- Knowledge of an appropriate OBC contact for additional template clarification and understanding.
- Familiarity with the RiskVision GRC tool and assessment process as it relates to plan assessment, authorization, and approval of ATO.

Plan Authors also require an understanding of VA System Inventory (VASI) and the Configuration Management Database (CMDB) to ensure proper access, use, and understanding of the specific infrastructure information for DRP development. The current CMDB training in

VA's Talent Management System (TMS) will be included as part of the virtual training and be updated accordingly.

Plan Reviewers are required to also have an understanding of the RiskVision GRC Tool in order to effectively use it as an evaluation tool and repository for DRP assessment results.

3.1.2.3 Identify and Recommend Test and Exercise

The TGT identifies and recommends disaster recovery testing and exercising for Plan Authors and Plan Reviewers. Testing will consist of

- Awareness of the Table Top Exercise (TTX) significance in the DRP process and how it is used to validate DRP viability. A TTX is a scripted scenario based testing of the operability of DRPs.
- Parameters for organizing and conducting a successful TTX.
- Understanding TTX results and they can improve the DRP.

Exercises will consist of

- Exercising TTX scenarios.
- Walking through a simulation of a disaster recovery scenario where a transfer of service of an application or system is required.

3.1.2.4 Identify Enterprise Criteria for Baseline DRPs

The TGT identifies enterprise criteria for DRPs that all Plan Authors will follow. Actions in the enterprise criteria will be performed sequentially and be retraced following the end of the DRP development or maintenance lifecycle. The enterprise framework includes the following steps for all Plan Authors:

1. Establish a BIA upfront. The output from the BIA should reflect proper recovery parameters. More details concerning BIAs can be found in VA BIA EDP⁴.
2. Access VASI and RiskVision GRC in order to assess the facilities' system inventory against existing information in VASI and RiskVision GRC with respect to appropriate recovery parameters.
 - a. Leverage applicable baseline information in both repositories to initiate DRP development or maintenance.

⁴ [VA OI&T ASD TS Business Impact Analysis Enterprise Design Pattern](#)

- b. Consider the mission criticality of the system, the type of system and facility the systems are hosted in (VA Medical Facilities [MCs], ITCs).
3. Access VA CMDB to keep track of all configuration items (CIs) such as operating systems, physical machines, virtual machines, and facilities. The CMDB provides insight into where the CIs are located and need to go in the event of a disaster: a primary hosting site or alternate failover site. For more information concerning CIs refer to VA Configuration Management (CM) EDP⁵.
4. Use information from VASI and CMDB to complete the DRP with respect to the OBC template.
5. Coordinate with Plan Reviewers at the facility level to perform quality assurance and approval review.
6. Disapproval by Plan Reviewers at the facility level prompts revision and resubmission by the Plan Authors.
7. Approval by Plan Reviewers at the facility level initiates coordination of the DRP with Plan Reviewers at the regional level.
8. Upon approval from the Plan Reviewers at the facility level and regional level, Plan Reviewers perform continuous monitoring of the DRP.
9. As systems inventory is updated onsite, plans are synced with VASI and CMDB. As a result, the DRP can refer to those repositories as the plan is being updated and benefit VASI and CMDB.
10. As part of continuous monitoring through coordination with the ISO, the DRP update needs to be tested prior to receiving ATO.

3.1.2.5 Apply Lessons Learned

The TGT will facilitate open discussion for developing and maintaining DRPs through a lessons learned platform. The objective of the platform is for DRP Plan Authors and Plan Reviewers to discuss and highlight best practices in the DRP lifecycle as well as to agree on areas for improvement. When results are shared beyond the teams of Plan Authors and Plan Reviewers, they enhance training competencies and increase plan compliance. The DRP Lessons Learned Information Sharing (LLIS) folder for enterprise DRP Lessons Learned will be in an accessible location for Plan Authors and Plan Reviewers. A potential location for the LLIS folder would be on the OBC portal. The LLIS platform promotes preparedness by identifying lessons learned and innovative practices, analyzing recurring trends, and sharing knowledge with the enterprise.

⁵ [VA OI&T ASD TS Configuration Management Enterprise Design Pattern](#)

3.2 AVAILABILITY OF AUTOMATION

3.2.1 Objective and Impact

A tool with automation capabilities would streamline and standardize the DRP development process, providing more consistent and accurate information within plans and “real-time” visibility into the progress of DRP development activities across the enterprise. Identified benefits with the use of automation include:

- Data mining capabilities for report generation and progress status information.
- Granularity in the reporting process between phases of plan completion.
- Ability to propagate template changes across multiple plans.
- Consistency in managing changes in the template and the information requested therein and propagation of changes to all related documents.

3.2.2 Approach

The automated tool should interface with systems, tools, and databases throughout the enterprise to effectively generate viable and testable DRPs. These enterprise resources are listed in Table 1.

Table 1: VA Resources for DRP Development

Terminology	Definition
VASI	An authoritative inventory of business-oriented applications and supporting databases that provides a comprehensive repository of basic information about VA systems; represents the relationships between systems and other VA data stores; and captures new systems.
CMS	A federated Configuration Management System (CMS) integrates multiple CMDBs into a single logical database. It creates a single federated environment where data stays in authoritative repositories that can be seamlessly accessed from external sources. Multiple Management Data Repositories (MDRs) are mapped to the CMS to improve communication between repositories. Additional information regarding CMS can be found in the Configuration Management EDP.
RiskVision GRC	The VA repository for housing completed DRPs.

Current private and commercial cloud offerings provide robust resources that VA will consider in a cloud based automated tool. Cloud tools can provide a quick, efficient, and low cost way of copying, moving, and maintaining data. A large percentage of the cost associated with disaster recovery planning comes from managing, moving, and maintaining the data. Automation

capabilities available through cloud tools can simplify DRP setup as well as testing and, through monitoring and reporting processes, identify incidents. Additional details on recommendations for Cloud Computing best practices within the enterprise can be found in the approved VA Cloud Computing EDPs.

Plan Authors would use the tool to populate the required fields within the DRP template to include technical restoration parameters such as Maximum Tolerable Downtime (MTD), Recovery Point Objective (RPO), Recovery Time Objective (RTO), operating system, restoration priority, alternate site location, and procedures etc. Once the template is completed, the tool relies on workflow generated notification intelligence to notify the next person in the review chain (System Owner, ISO, EM, EP Division Chief) that a plan has been completed and ready for review.

If the reviewer rejects the plan, then it is routed back to the Plan Author who developed the plan to correct and resubmit. Ultimately when the plan approval process is completed, the plan is forwarded to the Plan Reviewer at the enterprise-level for final review and submission into RiskVision GRC.

The tool would also provide leadership a clear enterprise-level view of the current state of disaster recovery planning. This is especially important when providing leadership with the past disaster recovery planning performance, current state, or forecasted future capabilities to inform Emergency Management decision making across the enterprise.

Additional benefits derived from using a tool with automation within the planning process include:

- Metrics on number and percent of plans completed.
- Metrics on when plans were started and progress towards completion.
- Metrics on whether plans are on track or will be submitted late.
- Surveys and reports can be tailored to meet specific needs of departments and management.
- Acknowledgement from designated POC that updated templates and action items have been received.
- Visibility of the review and approval flow as the plan progresses through the development process.

3.3 ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM)

The [VA Technical Reference Model \(One-VA TRM\)](#) is a component within the overall enterprise architecture that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications.

All ITSM products used to realize disaster recovery planning principles in this document require approval in the TRM. The approved products refer to the ITSM tools that constitute the framework described in the ITSM Enterprise Framework EDP. Table 2 shows a representation of the current approved products for pertinent ITSM categories.

Table 2: Representative VA ITSM Enterprise Framework Categories and TRM-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
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 (VASI)
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
Enterprise and Service Architecture Design Tooling	Rational System Architect and Rational Software Architect

3.4 ALIGNMENT TO VETERAN-CENTRIC INTEGRATION PROCESS (VIP)

The Veteran-focused Integration Process (VIP) is the follow-on framework from Project Management Accountability System (PMAS) for the development and management of IT projects which will propel VA with even more rigor toward Veteran-focused delivery of IT capabilities. VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP framework unifies

and streamlines IT delivery oversight and will deliver IT products more efficiently, securely, and predictably.

All projects subject to VIP require an ATO using the Assessment and Authorization process in ProPath. The ATO is driven by evaluations of security controls that are determined based on an understanding of business needs and mission criticality, which is supported by the BIA.

More information can be found here (<https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/>).

4 USE CASES

4.1 USE CASE 1 – APPLYING VA ENTERPRISE TGT OVERSIGHT

4.1.1 Purpose

This use case demonstrates how VA Enterprise TGT, as described in section 3.1.1 of this document, effectively assists in closing knowledge gaps for Plan Authors and Plan Reviewers in the disaster recovery planning process. The TGT possesses understanding and an intimate knowledge of appropriate VA disaster recovery planning resources, their locations, and how to implement them. Resources such as the VA Talent Management System (TMS), the OBC portal, and any new locations identified in the updated VA Handbook 6500.8 are essential to Plan Authors and Plan Reviewers for completing DRPs.

4.1.2 Assumptions

- TGT members have a full understanding of the new VA Handbook 6500.8 policy changes, know how to effectively implement it into the disaster recovery planning process, and know where to locate related resources.
- The updated VA Handbook 6500.8 policy is available and accessible to Plan Reviewers and Plan Authors on the OBC portal.
- TMS courses related to disaster recovery planning reflect updated policy information and are available and accessible for self-paced training for all Plan Reviewers and Plan Authors.
- Plan Reviewers and Plan Authors have access to RiskVision GRC, VASI, and the CMDB as appropriate by role.
- The finalized facility DRP due date is more than 5 months away.

4.1.3 Use Case Description

A recent update of VA Handbook 6500.8 policy for disaster recovery planning was published for implementation during the next DRP update. The policy update relates to a technology change and directly affects the type of information that is necessary for Plan Authors to complete the DRP template. Failure to adhere to the policy change will result in poor viability and non-compliant plans.

Step 1

OBC informs the TGT, Plan Reviewers, and Plan Authors of the VA Policy update related to the disaster recovery planning process. OBC performs the following actions to prepare resources for the TGT to standardize guidance while implementing the VA Handbook 6500.8 Policy update.

- Revise the DRP Template to reflect updated VA Policy.
- Upload a copy of the VA Policy and DRP template, and provide links for TMS-related training courses onto the OBC portal.
- Provide a timeline of due dates for the finalized plan and progression milestones.

Step 2

Plan Reviewers and Plan Authors receive a list of responsibilities by role (ISO, System Owner/SME, Ems, and EP Division Chief) for awareness of their accountability to the plan development process. To fully understand their roles, Plan Reviewers and Plan Authors complete role-based training using the TMS, and access RiskVision GRC, VASI, and the CMDB, as appropriate by role, to fully participate in the DRP planning and execution lifecycle.

Step 3

Establish a workflow plan, developed by the TGT and communicated to Plan Reviewers and Plan Authors, based on core guidelines and criteria for updating the DRPs that are in sync with the updated VA Handbook 6500.8.

Step 4

Following DRP development by Plan Reviewers and Plan Authors, the TGT submits and promotes their thoughts on the process lifecycle in the VA LLIS folder on the OBC portal. The TGT maintains the responsibility of facilitating discussions of what went well during the DRP lifecycle and areas that the Plan Authors and Plan Reviewers would like to adjust or improve.

The LLIS data is maintained to improve and inform future disaster recovery planning processes and outcomes.

4.2 USE CASE 2 – WORKFLOW AUTOMATION SUPPORT FOR DRPS

4.2.1 Purpose

The purpose of this use case is to describe how tools containing workflow automation can streamline development of DRPs, leveraging functionality described in Section 3.2.1 of this document. The tool enables users to identify IT assets in disparate OI&T repositories, and it provides the ability to review progress toward developing and maintaining the DRPs. The DRPs are ultimately stored in RiskVision and reviewed by the ISO to maintain an ATO, and are reviewed by system owners to ensure that IT systems continue to maintain Service-level Agreements (SLA) in the event of a disaster.

4.2.2 Assumptions

- A completed and approved ISCP document provided by the business owners is accurate and contains the required and approved BIA information.
- Technical details required for insertion into the DRP have been established.
- The DRP template used is the most current approved version.
- Sufficient data recovery capacity has been identified.
- An ISO with authority is available to make decisions on plan completeness and viability.

4.2.3 Use Case Description

This use case describes a scenario that involves the use of tools that automate some of the data gathering required to develop a complete DRP. This scenario takes into account a set of virtual servers that constitute an IT system hosted at a VA ITC, with failover to another ITC in the event of a disaster. The tool helps keep track of the system's CIs efficiently and helps the system owner accurately manage the SLA.

Step 1

An IT infrastructure SME, designated by the System Owner, opens the approved/updated DRP template provided by OBC. The template includes multiple pull-down boxes that will allow the SME to select likely pre-populated responses for particular field in the template. This will support consistent responses from SMEs and increase the reliability of the information captured.

Step 2

The delegated SME for the System Owner leverages the tool to obtain CI information from the CMDB to help populate the DRP. The CMDB will automatically populate CI information about the virtual servers, including:

- The name of the server.
- Server operating system.
- Programs that will run on the server.
- Memory and data storage information.
- System and supporting component restoration priorities.
- Alternate processing procedures and alternate site location.

The tool automatically mines for technical restoration parameters such as MTD, RPO, and RTO established during benchmark testing of the system that are also identified in the template.

Step 3

Once the SME fully populates the template and conducts initial DRP testing, the SME passes on the DRP for review and approval to either of the following;

- The System Owner identified for the facility/site submitting the DRP.
- The leader of the Emergency Management team responsible for the facility.

The tool integrates with RiskVision and gives a reporting status update to the stakeholders involved in the DRP completion and approval.

Step 4

If the plan is reviewed and approved by the System Owner or Emergency Management team lead, he/she will notify the ISO electronically that a site/facility DRP is ready for review and approval.

If the System Owner does not concur with the information in the DRP, he/she will reject the DRP and send it back to the SME for correction or updating.

Step 5

The SME will review and address the comments provided by the System Owner or Emergency Management lead and use the tool to propagate changes to the appropriate CI attributes from the CMDB. The SME does not require manual review of each CI, rather one correction is propagated across all of the CIs referenced in the DRP. Additionally, the tool recognizes references to the DRP in other plans that are included in RiskVision, and it automatically propagates changes across other plans that have DRP references. The SME completes the DRP

based on the automated gathering of the information from the CMDB and system attributes referenced in the VASI. The SME will then resubmit the plan for review and approval.

Step 6

Assuming the plan is approved by the System Owner or Emergency Management lead it will be forwarded to the ISO for review and approval. DRP stakeholders are able to check the status of the DRP through RiskVision.

Step 7

If the ISO does not approve of the plan they will reject it and send it back to the system owner or Emergency Management team lead for corrective action. The System Owner, with help from the SME who authored the plan, will address the concerns of the ISO and resubmit for his or her approval. If the resubmitted plan is approved, then it is sent along to the facility Chief Information Officer (CIO) who acts as the next approver in the approval chain.

Step 8

If the final approver approves the plan, then it will be forwarded to OBC for archival in a database that can be queried by those involved in DRP development and disaster recovery restoration activities. If the DRP is not accepted, it will be returned to the System Owner for review and editing as required. The DRP will then be re-submitted by the ISO for review and approval.

APPENDIX A: SCOPE

This Enterprise Design Pattern (EDP) provides an enterprise-level view of the “As-Is” and “To-Be” DRP capabilities relevant to VA. The document will refer to, rather than duplicate, lower-level solution guidance associated with these capabilities.

This EDP focuses on:

- Current DRP capabilities and constraints at VA.
- Guidance that ensures a framework for bridging the gaps in governance and automation for DRPs.
- A set of use cases that will allow VA to leverage governance and automation opportunities for DRPs.
- The EDP document is generally applicable across all VA Lines of Business (LOB) and describes:
 - “As-Is” VA DRP capabilities.
 - Processes for use by those that execute DRP responsibilities at VA.
 - Enterprise-level DRP constraints, strategic guidance, and terminology.

This EDP document **does not** address detailed technical solution guidance for implementing specific mobile applications. It will only provide the constraints to drive DRP towards development of solutions that effectively meet the specific goals of their initiatives.

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

- Contingency Planning (also referred to as Information System Contingency Planning)
- Continuity of Operations (COOP) Planning
- Business Continuity Planning (BCP)
- Business Impact Analysis (BIA)
- Recovery of facilities

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across the Department and included participation from VA’s Office of Information and Technology (OI&T), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA). In addition, the development effort 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.

APPENDIX B: DEFINITIONS

Terminology	Definition
Business Continuity Planning (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
Business Impact Analysis (BIA)	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Contingency Planning	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. Information system contingency planning refers to the dynamic development of a coordinated recovery strategy for information systems, operations, and data after a disruption.
Continuity of Operations (COOP) Plan	A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.
Critical Business Process (CBP)	The operational and / or business support functions that could not be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing the organization.
Disruption	An unplanned event that causes an information system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
Disaster Recovery Plan (DRP)	A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. The DRP is supported by the information system contingency plans (ISCPs) for each critical IS Service at the affected facility.
Governance, Risk, & Compliance (GRC)	Software utilized by VA to track documentation related to risk. The documentation and artifact requirements in RiskVision GRC must be completed and reviewed by required staff (ISOs) prior to either type of visit. If you do not have this completed, problem with completing or answering questions will occur.

Terminology	Definition
Information Security Contingency Plan Assessment (ISCPA)	The nine-step process for contingency planning within VA.
Information System (IS)	An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, and control data or information. An information system will consist of automated data processing system hardware, operating system and application software, peripheral devices, and associated data communications equipment.
Information System Contingency Plan (ISCP)	A written plan describing the coordination activities between the primary, and recovery site(s) that are required to recover and continue IS service operations. ISCPs for each IS Service are referenced in the Disaster Recovery Plan (DRP) in order to assist in the restoration of critical systems or transfer of critical systems' data to the recovery site after it has been appropriately configured.
Recovery Site	A location, other than the systems primary location, used to continue operational capabilities during a significant system disruption.
Risk Based Decision (RBD)	A required document that identifies a risk and the compensating controls to mitigate a risk that cannot be remediated.
Site Readiness Assessment (SRA)	SRA's are site visits conducted by the ERM Team, lasting 3 days.
System	A generic term used for brevity to mean either a major application or a general support system.
Table Top Exercise (TTX)	A facilitated discussion of a scripted scenario in an informal, practice environment. A TTX is designed to elicit discussion as participants examine and resolve problems based on existing operational plans and identify where those plans need to be refined.
Tabletop Exercise (TTX) After Action Report (AAR)	Captures the performance during the Table Top Exercise (TTX) exercise. It identifies strengths to be maintained, potential areas for improvement, and supports tracking the progress of corrective actions.

Terminology	Definition
Test	An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an ISCP.
Test Plan	A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step.
User	A person who accesses information systems to use programs or applications in order to perform an organizational task.
VA Handbook 6500.8	This Handbook provides the specific procedures and operational requirements for implementing IS contingency planning in accordance with VA Directive and Handbook 6500, Information Security Program, ensuring Department-wide compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-3549 and the security of VA information and information systems administered by or on behalf of VA. This handbook applies to all VA organizations, their employees, and contractors working for or on behalf of VA. This Handbook includes revisions based on the NIST SP 800-34 (Rev. 1) Contingency Planning Guide for Federal Information Systems.

APPENDIX C: ACRONYMS

Acronym	Description
ASD	Architecture, Strategy, and Design
ATO	Authority to Operate
BC	Business Continuity
BIA	Business Impact Analysis
CI	Configuration Item
CIO	Chief Information Officer
CMDB	Configuration Management Database
CMS	Configuration Management System
DRP	Disaster Recovery Plan
EDP	Enterprise Design Pattern
EM	Emergency Manager
EMT	Emergency Management Team
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
GRC	RiskVision Governance, Risk, and Compliance
ISCP	Information System Contingency Plan
ISCPA	Information System Contingency Planning Assessment
ISO	Information Security Officer
IT	Information Technology
ITC	Information Technology Center
ITSM	Information Technology Service Management
ITWD	Information Technology Workforce Development
LLIS	Lessons Learned Information Sharing
MEF	Mission Essential Function
MTD	Maximum Tolerable Downtime
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
OBC	Office of Business Continuity
OI&T	Office of Information and Technology
OPA	Office of Personnel and Accounting
PAID	Personnel and Accounting Integrated Data
PD	Product Development
PMAS	Project Management Accountability System
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service-level Agreement
SMART	Security Management and Reporting Tool
TMS	Talent Management System
TRM	Technical Reference Model

Acronym	Description
TTX	Table Top Exercise
VA	Department of Veterans Affairs
VASI	VA System Inventory
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VIP	Veteran-Centric Integration Process

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 the VA, and are aligned to the VA ETA:

#	Issuing Agency	Applicable Standard	Reference/ Purpose
1	VA	VA Directive 6551	Establishes a mandatory policy for establishing and utilizing Enterprise Design Patterns by all Department of Veterans Affairs (VA) projects developing information technology (IT) systems in accordance with the VA's Office of Information and Technology (OI&T) integrated development and release management process, the Veteran-focused Integration Process (VIP).
2	NIST	NIST 800-34, Rev. 1, <i>Contingency Planning Guide for Federal Information Systems</i>	Focuses on restoring an organization's mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations
3	VA	VA Handbook 6500.8, <i>Information System Contingency Planning</i>	This Handbook provides the risk-based process for selecting VA information technology system security controls and operational requirements to implement VA Directive 6500, an updated VA National Rules of Behavior, and an appendix addressing VA privacy controls. The Handbook is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

APPENDIX E: VA DRP POLICIES AND DIRECTIVES

Policy/Directive	Year
Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix III	November 2000
Department of Homeland Security (DHS), National Security Presidential Directive 51 / Homeland Security Presidential Directive 20, National Continuity Policy	May 2007
DHS, Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements	October 2012
DHS, National Response Framework	May 2013
DHS, Homeland Security Exercise and Evaluation Program (HSEEP)	April 2013
Homeland Security Council, National Continuity Policy Implementation Plan	August 2007
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, Contingency Planning Guide for Information Technology Systems	May 2010
NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations	January 2014
NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	September 2006
VA Handbook 6500.8, Information Technology Contingency Planning	April 2011
OI&T Comprehensive Emergency Management Homeland Security Test, Training & Exercise Program Strategy (Draft)	January 2010
Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix III	November 2000

APPENDIX F: ISCPA PROCESS

