VA Enterprise Design Patterns:

IT Service Management (ITSM)

Contingency 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 E. Marshall 137891

Digitally signed by Gary E. Marshall 137891
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=gary.marshall@va.gov, cn=Gary E. Marshall 137891
Date: 2016.11.09 13:59:15 -05'00'

Gary Marshall
Director, Technology Strategies, ASD

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: 2016.11.15 17:42:13 -05'00'

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

REVISION HISTORY

Version	Date	Organization	Notes
0.1	7/15/16	ASD TS	Initial Draft/Outline
0.3	8/2/16	ASD TS	Updated introduction, current capabilities, future capabilities, and initial draft of use cases.
0.5	9/6/16	ASD TS	Refined future capabilities, updated use cases.
0.7	10/6/16	ASD TS	Updates made following Public Forum collaborative feedback and working session.
1.0	10/7/2016	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	7/26/16	Jacqueline Meadows-Stokes	Enterprise Design Pattern Lead
0.3	8/9/16	Jacqueline Meadows-Stokes	Enterprise Design Pattern Lead
0.5	9/13/16	Jacqueline Meadows-Stokes	Enterprise Design Pattern Lead
0.7	10/6/16	Jacqueline Meadows-Stokes	Enterprise Design Pattern Lead

TABLE OF CONTENTS

FIGURES

TABLES

1 INTRODUCTION

Many business functions within Department of Veteran Affairs (VA) are dependent on Information Technology (IT) systems. These include benefits claims processing, disbursement allocation, burial arrangements, and health records. Interruptions and disruptions to these systems could delay:

- Health claims processing
- Disability disbursement
- Effective treatment of patients by VA physicians
- Burial of a Veteran

To ensure that these business functions continue, it is imperative to assess, plan for, and react to disruptions to systems that support these important services and functions. Contingency planning will "mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability."[1] VA must withstand all hazards and sustain its services and functions through many different changes.

The purpose of this Enterprise Design Pattern (EDP) is to provide guidance to VA projects on effective contingency planning for IT systems within the VA enterprise. This guidance will include measures and recommendations that will address compliance, tool usage and automation, governance and policy requirements, and training.

1.1 BUSINESS PROBLEM

In October 2011, VA implemented the Office of Information and Technology (OI&T) Annual Security Calendar, requiring all Information System Contingency Plans (ISCP) and Disaster Recovery Plans (DRP) be updated on an annual basis. However, the 2015 VA Office of Inspector General (OIG) audit of VA's information security programs and practices identified weaknesses in contingency planning efforts similar to those identified in FYs 2012 and 2013 audits. The 2015 VA OIG audit included the following findings for contingency planning[2]:

- VA contingency plans were not always fully documented
- Some ISCPs were not updated to reflect detailed disaster recovery procedures for all system components or reflect current operating conditions

These findings reveal issues with governance, oversight, and policy as it relates to contingency planning. While VA mandates contingency planning for all its information systems, it is not

[1] NIST 800-34, Rev. 1
[2] VA OIG FISMA Audit FY15

globally enforced. The inconsistent, outdated, and incomplete plans reveal an enterprise-level training issue.

1.2 BUSINESS NEED

This EDP will identify contingency planning gaps within VA and recommend best practice for bridging those gaps. The document can be used to:

- Evaluate and update existing policies, and create new policies which will provide the authority and guidance necessary to mandate developing and maintaining effective contingency plans
- Develop comprehensive recovery strategies so that systems can be recovered quickly and effectively following a disruption
- Streamline the current ISCP assessment process required for all systems deemed "Federal Information Security Management Act (FISMA) High"[3]. While FISMA High systems are required, FISMA Medium and FISMA Low systems do not require contingency plans. System owners of FISMA Medium and Low systems can choose to develop contingency plans based on business needs
- Create an evaluation methodology that assesses the completeness of contingency plans

1.3 BUSINESS CASE

This EDP will increase the readiness posture of VA IT systems and ensure continued services and functions. This will ultimately ensure that the Department is fulfilling its mission, "To care for him who shall have borne the battle, and for his widow, and his orphan." This EDP provides positive outcomes to the business benefits outlined in Table 1.

Table 1 - Business Benefits

Business Benefits	Description
Appropriate oversight of contingency plan completion and maintenance	Appropriate governance and accountability to ensure that systems are ready and prepared for disruption. This means all FISMA High systems have been identified, assigned to owners, and have completed contingency plans.

[3] Per FIPS 199, FISMA High systems are information systems categorized as high- including impact for the security objectives of confidentiality, integrity or availability require contingency plans.

Business Benefits	Description
Appropriate planning for timely restoration of systems and appropriate testing	Accurate planning data and processes enable systems to be restored quickly and efficiently and tested regularly.
Highly trained system owners	Prepares system owners to complete contingency plans and update them annually or as major changes occur in accordance with National Institute of Standards and Technology (NIST) 800-34, Rev. 1. This ensures that systems owners are aware and trained for appropriate contingency planning procedures.

1.4 APPROACH

Solutions for bridging contingency planning gaps within VA include:

- Ensuring authoritative oversight of contingency planning throughout the enterprise
- Establishing evaluation criteria to determine a contingency plan's compliance with NIST 800-34, Rev. 1 and VA Handbook 6500.8
- Leveraging a best practice tool that:
    - Interoperates with the Information System Contingency Planning Assessment (ISCPA)
    - Assesses contingency planning within VA
    - Flags outdated or incomplete system information
- Incorporating a training program that better prepares system owners for the contingency planning assessment process

2 CURRENT CAPABILITIES

VA has several processes, policies, and programs in place for contingency planning. The following section describes the current capabilities for contingency planning within the enterprise.

2.1 INFORMATION SYSTEM CONTINGENCY PLAN (ISCP)

VA's ISCP is a manual process that reports and stores contingency plans. This process identifies contingencies for circumstances, events, or acts that could cause harm to systems by

destroying, modifying, or denying access to information resources. It also provides flexible and scalable recovery strategies to accommodate a variety of disruptions. It is critical that services provided by VA are able to recover operations effectively without excessive interruption.

One of the goals of the ISCP is to establish procedures and mechanisms that obviate the need to resort to performing IT functions using alternate methods. If alternate methods are the only option during a disruption, every effort must be made to continue IT functions and processes manually. The nature of unprecedented disruptions can create confusion, and often predisposes an otherwise competent IT staff towards less efficient practices. In order to maintain a normal level of efficiency, it is important to document notification and activation guidelines and procedures, recovery guidelines and procedures, and reconstitution guidelines and procedures prior to the occurrence of a disruption. During the notification/activation phase, appropriate personnel are apprised of current conditions and damage assessment begins. During the recovery phase, appropriate personnel take a course of action to recover the systems components a site other than the one that experienced the disruption. In the final phase, reconstitution, actions are taken to restore IT system processing capabilities to normal operations.

The plan contains background information including:

- The description of the system being assessed
- The roles and responsibilities of the personnel involved in implementing the plan
- Document ownership
- Personnel contact data
- Call trees
- Recovery site information
- Alternate storage and processing procedures, and
- A Business Impact Analysis (BIA)

Additionally, the plan covers procedures for activation and notification, recovery, and reconstitution. To ensure the plan is exercised and evaluated annually, detailed procedures for Test, Training, and Exercise (TT&E) are also outlined within the ISCP.

This process was once automated, providing both a template and a step-by-step process for contingency planning completion. Due to security concerns, the system was decommissioned. Returning to a manual process has led to inconsistencies in completing contingency plans. This resulted in incomplete, outdated, and incorrect contingency plans.

2.2 INFORMATION SYSTEM CONTINGENCY PLANNING ASSESSMENT (ISCPA)

The ISCPA is used to identify and document all existing backup, business continuity, and disaster recovery plans—collectively referred to as contingency plans. The assessment identifies and maps contingency planning requirements through development of a BIA and threat and vulnerability analyses. This mapping will:

- Gather business requirements
- Map components to services
- Identify and prioritize threats
- Identify threat-related vulnerabilities and prioritize services

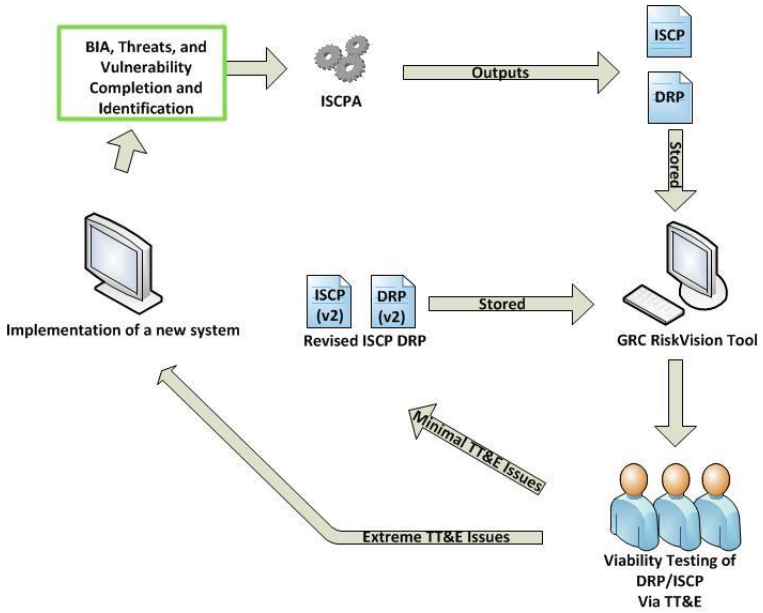

Figure 1: ISCPA Process Graphic

While the assessment provides critical information necessary to making investment decisions, stakeholder feedback reveals that ISCPA rarely results in investments. Per the ISCPA, services and systems possessing a "high critical exposure rating" are required to have written ISCP and Disaster Recovery Plans (DRP). These plans support key decisions within VA as they relate to investment and recovery strategies, procedures, and infrastructure.

2.3 VA HANDBOOK 6500.8, INFORMATION SYSTEM CONTINGENCY PLANNING

In 2011, VA Handbook 6500.8, *Information System Contingency Planning,* was published to supersede the prior version. This handbook includes specific procedures and operational requirements for contingency planning in accordance with VA Directive and Handbook 6500,

Information Security Program. VA Handbook 6500.8 also cites system owners, regional directors, and data center directors with responsibility for ensuring compliance with the ISCPA process and providing oversight for completeness. While the policy establishes governance of the contingency planning process and encourages enterprise-wide compliance with federal requirements and NIST recommendation, there are notable inconsistencies regarding how contingency plans are completed and maintained. This inconsistency in contingency plan development and upkeep is driven by the lack of clear, authoritative oversight at the enterprise level.

2.4 INFORMATION TECHNOLOGY WORKFORCE DEVELOPMENT TRAINING

VA Handbook 6500.8 mandates that "system or facility owners train personnel in their contingency roles and responsibilities, with respect to moderate and high impact information systems, and provide a refresher training at least annually." VA Handbook 6500.8 also states that "all ISCPs and DRPs will be tested annually and when major organizational, operational, procedural, or technical changes are made."

The FISMA Audit for FY-2015, Finding 5, revealed that "VA contingency plans still were not fully documented or reflective of current operating environments." These inconsistencies are due in part to a lack of consistent training for system owners within the VA enterprise. There is a web-based training on the IT Workforce Development (ITWD) Talent Management System (TMS) that could be used to train contingency planning personnel. There is no enterprise-wide mandate to complete this training.

3 FUTURE CAPABILITIES

Table 2 - Mapping of Future Capabilities of Business Problems

Capability	Description
Automation Tool for ISCP Plan and Process	Implementing a tool that automates the process would mean a more efficient, consistent process for completing contingency plans. The tool also could be programmed to flag both incomplete and outdated contingency plans.
Contingency Planning Policy Update	Revising of VA Handbook 6500.8, *Information System Contingency Planning,* is necessary to assign clear enterprise oversight to contingency planning.

Capability	Description
Required Training for Contingency Planning Support Staff	Require system owners to be trained both consistently and annually.

3.1 AUTOMATING THE INFORMATION SYSTEM CONTINGENCY PLANNING ASSESSMENT

The Office of Business Continuity (OBC) regulates and oversees the ISCPA process, and requires that all systems deemed "FISMA High" complete an ISCP at least annually. This 40-page report requires system owners to:

- Determine threats, threat values, vulnerability, vulnerability rating, impact value, and exposure value
- Provide scope and assumptions for the contingency plan
- Weigh threats against likelihood
- Provide an overview of the activation and notification, recovery, and reconstitution of the affected system
- Provide an inventory of components
- Outline the system interconnections
- Describe in detail the roles and responsibilities for the execution or support of system recovery
- Require an outage assessment
- Require an outline of the associated TT&E program
- Provide information on management of the ISCP document

Automating this process will increase oversight ensuring plans are both complete and up-to-date. Automation will provide some consistency with contingency planning within the VA enterprise, decrease duplicate information, and allow for consistent evaluation and review of contingency plan compliance.

A large percentage of the cost associated with contingency planning comes from managing, moving, and maintaining data. Automating data management by using a cloud-based data management tool will minimize costs. A cloud-based tool will translate to minimal storage burden on the VA infrastructure. Leveraging cloud services will also simplify requirements for TT&E activities, easing contingency plan completion requirements while minimizing costs. There are several approved EDPs that provide recommendations for cloud computing best practices within the enterprise.

3.2 UPDATE OF THE VA ENTERPRISE CONTINGENCY PLANNING POLICY

VA Handbook 6500.8 requires that "completed and updated information system contingency plans (ISCPs) and disaster recovery plans (DRPs) are uploaded into the Security Management and Reporting Tool (SMART) database." This database has since been replaced by RiskVision Governance Risk and Compliance (GRC) to manage and mitigate enterprise-wide risk and security management.

VA Handbook 6500.8 needs review and revision to take into account changes in the NIST guidance and updates to the systems used to manage risk and security. This revision will ensure that the appropriate measures are considered and implemented to protect the information and information systems within the department.

3.3 TEST, TRAIN, AND EXERCISE FOR CONTINGENCY PLANNING

Contingency planning within VA requires:

- Comprehension of policies and guidance that regulate contingency planning in the federal government
- Knowledge of operational requirements for VA IT services, disaster recovery planning, and mission essential function (MEF) continuation; and
- Constant testing and revision of plans and procedures for the recovery of critical systems and processes

It is imperative that personnel involved in developing contingency plans are trained in contingency planning. At present, there is a web-based training on the TMS that provides introductory information and scenario based training for contingency planning and is available to all employees. Distance or in-person role-based training by Subject Matter Experts (SMEs) at the facility or regional levels would supplement the scenario-based training offered. This training provides valuable insight for personnel involved in contingency planning and should be an annual requirement.

3.4 ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM)

All projects will leverage the approved tools and technologies located in the VA Technical Reference Model (TRM)[4] to comply with the architectural guidance provided in this document. Table 3 lists the approved tools for this EDP.

[4] http://trm.oit.va.gov/

Table 3 - List of Approved Tools and Standards for Enterprise Authorization

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

3.5 ALIGNMENT TO VETERAN-CENTRIC INTEGRATION PROCESS (VIP)

Veteran-Centric Integration Process (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. Prior to achieving an Authority to Operate at Critical Decision 2, projects are required to develop contingency planning to address availability, and to develop ISCPs, as required by the Information Security Officer. More information can be found here.

4 USE CASES

4.1 VA MEDICAL CENTER POWER OUTAGE

4.1.1 Purpose

A recent power outage of the VA Medical Center prompted an initial audit of the hospital's contingency plans. The findings of the initial audit resulted in:

- A "stand-up" of an Enterprise Working Group, housed under OI&T, to determine contingency priorities
- The review/revision of 6500.8 Governance Handbook to assign regional contingency planning oversight
- The creation of a contingency planning training program in IT Workforce Development
- The utilization of a tool that identifies deficiencies in contingency planning for VA Medical Facilities throughout the enterprise

4.1.2 Assumptions

- Existing generators malfunctioned and are not an option for backup power
- VistA is one system that is down due to the power outage. VistA provides an integrated inpatient and outpatient electronic health record for VA patients, and administrative tools to help VA deliver the best quality medical care to Veterans
- After a Major Outage[5], the local Power and Light Company prioritizes the following: Public safety by restoring power to critical services like hospitals, police and fire stations, and water treatment plants
- The VA Medical Center possesses viable contingency plans that describe procedures for backing up records and/or workarounds until power is restored
- Manual processing will occur for critical functions until power is restored

4.1.3 Use Case Description

A storm related power outage with high winds resulted in tree branches and limbs making contact with power lines. The VistA Imaging System lost power and cannot be restored due to a failed generator. This required the activation of the VistA Imaging System Contingency Plan in order to restore the system.

The impact to the loss of the VistA System includes the inability for Veteran doctors to adequately treat patients. This means the inability for VA to adequately perform the Primary Mission Essential Function (PMEF).

[5] As defined by VA Handbook 6500.8

A Contingency Planning Working Group (CPWG) was stood up to:

- Outline contingency planning priorities
- Review the existing contingency planning policy and provide recommendations for improvement
- Develop contingency planning training in IT Workforce Development; and
- Identify tool requirements to ease contingency plan development

Contingency planning priorities are those aspects that affect VA enterprise operations. The priorities are contained in the table below.

Table 4- Contingency Priorities Table

Level 1 Contingency Priorities	• Systems that support PMEF (medical care, treatment, hospitals) • Systems that support emergency response • Systems that aid in devolution and reconstitution
Level 2 Contingency Priorities	• Systems that affect personnel accountability
Level 3 Contingency Priorities	• All other systems

Leadership will use these priorities to make informed decisions about investment strategies, recovery prioritization, alternate system planning, and budgets.

Additionally, the committee reviewed VA Handbook 6500.8 and provided recommendations to ensure that the policy was adequate and up-to-date for the enterprise. Key stakeholders, contingency planners, and leadership review the new policy.

Staff that write contingency plans provide support during contingency plan activation. Leadership should also be trained in contingency planning. A storyboard for a proposed training was created by the CPWG subcommittee on contingency planning and submitted to ITWD for development. Leadership is creating a mandate that all personnel affected by contingency plans take this training annually or as needed to perform role duties.

To ensure consistency among contingency plans throughout the enterprise, a set of requirements for a tool was developed. The requirements include:

1. An automated completion process
2. The detection/flagging of outdated plans, systems, or software
3. A tool that generates a printable report
4. A tool that is compatible with the existing ISCP
5. Cloud-based data management capabilities

VA will use these requirements to determine an eligible tool to acquire.

Full details of the use case description and a related business impact analysis are located in Appendix F and Appendix G respectively.

4.2 OFFICE OF PERSONNEL AND ACCOUNTING BUSINESS IMPACT ANALYSIS FOR THE CONTINGENCY PLAN PROCESS REVIEW

4.2.1 Purpose

The Office of Personnel and Accounting recently completed a BIA in preparation for the development of contingency plans. This BIA will determine criticality level and planning requirements for system recovery and alternatives. Based on information captured in the BIA, a contingency plan for the identified system/application will be developed.

4.2.2 Assumptions

- The Office of Personnel and Accounting (OPA) has identified all of their MEF systems
- Risk levels have been established for each MEF
- MEFs may or may not have existing contingency plans for critical mission systems

4.2.3 Use Case Description

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business processes the system supports, and using this information to characterize the impact on the processes if the system were unavailable. The BIA is composed of the following three steps:

1. Determine the mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime reflects the maximum that an organization can tolerate while maintaining the mission
2. Identify resource requirements. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources to identify include facilities, personnel, equipment, software, data files, system components, and vital records
3. Identify recovery priorities for system resources. Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources

The information listed in the table below was captured from the full BIA document for the Personnel and Accounting Integrated Data (PAID) system which can be found in Appendix B.

Table 5-PAID System BIA

Personnel and Accounting Integrated Data (PAID) Business Impact Analysis	
Description	This is the payroll and human resource system for managing payroll services for employees across VA
System Owner	CIO of the OPA
Critical Business Process	Updating of databases for personnel actions affecting payroll
MTD	12 hours, based on the need of the Employee to be paid
RTO	12 hours
MTD-RTO GAP	0 hours
RPO	2 hours
Alternate Procedures	There is no alternate process for updating the data in PAID when the application (OLDE/Edit & Update) is unavailable. Alternate processing procedures for payroll processing include: DFAS can be notified to pay everyone a “straight 80” hour pay. Stations could communicate with DFAS to create Remedy tickets to pay new employees.

APPENDIX A. SCOPE

The purpose of this Enterprise Design Pattern (EDP) document is to provide guidance to VA stakeholders on effective contingency planning within the VA enterprise.

This document will address current VA contingency planning gaps including:

- Compliance measures with VA Handbook 6500.8 and NIST 800-34, Rev. 1
- Implementation of existing tools/resources available to VA for contingency plan completion and evaluation
- Governance or policy clearly outlining contingency planning oversight within VA
- Training of system owners on appropriate contingency planning

This EDP **does not** address detailed solution guidance for creating enterprise level contingency plans or tools/products that will offer solutions to OIG findings. This document will provide the constraints to drive contingency planning and support towards the development of solutions throughout the enterprise.

Topics falling outside of the scope of this EDP but possibly referenced are:

- Continuity of Operations Planning
- Disaster Recovery Planning
- Business Impact Analysis
- Business Impact Analysis Maintenance

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across the Department and included participation from VA 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 Veteran Health Administration (VHA), Veteran Benefits Administration (VBA), and National Cemetery Administration (NCA). In addition, the development effort included engagements with industry experts to review and provide input on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. The Government lead for this document coordinates updates, which also facilitates stakeholder coordination and subsequent re-approval depending on the significance of the change.

APPENDIX B. OFFICE OF PERSONNEL AND ACCOUNTING BIA

Business Impact Analysis
Office of Personnel and Accounting
Personnel and Accounting Integrated Data (PAID) System
FIPS 199 Overall Impact Level = High
FIPS 199 Availability Security Categorization = High

The Office of Finance is responsible for continually improving the quality of the Department's financial services. It maintains stewardship of Departmental resources and provides financial information, financial statements and reports on VA's appropriations and general, revolving, special, and deposit funds for cost and obligation accounting. The Office of Finance establishes financial policy, systems and operating procedures for all VA financial entities, provides guidance on all aspects of financial management, and directs and manages the Department's financial operations and systems support.

The office is also responsible for maintenance and modification of VA's legacy core accounting system, the Financial Management System (FMS), and VA's Personnel Accounting Integrated Data (PAID)/payroll and human resources system and related self-service applications.

Assumptions:

- OPA has identified all of their MEF systems
- Risk levels have been established for each MEF
- MEF's may or may not have existing contingency plans for critical mission systems

Background:

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business processes the system supports, and using this information to characterize the impact on the processes if the system were unavailable. The BIA is composed of the following three steps:

1. *Determine the mission/business processes and recovery criticality.* Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. Ideally, downtime reflects the maximum that an organization can tolerate while still maintaining the mission

2. *Identify resource requirements.* Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources to identify include facilities, personnel, equipment, software, data files, system components, and vital records
3. *Identify recovery priorities for system resources.* Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources

Identify Critical Business Processes:

1. Enter the critical business processes (CBPs) that depend on the IS. Note: A CBP is an operational and/or business support function that cannot be interrupted for more than a mandated or predetermined timeframe without significantly jeopardizing the organization/mission
2. Create additional rows as needed to accommodate all CBPs that depend on the IS

Table B-1: Critical Business Processes
1. Update Online Data Entry (OLDE) database to reflect the latest personnel changes
2. Process personnel actions through PAID (Edit and Update process)
3. Interface personnel data for time reporting in VATAS

Identify Service/Business Lines and Determine Maximum Tolerable Downtime:

A. Service/Business Lines
    1. Enter the Service/Business Lines that use the CBPs. Note: A service/business line is a segment of a VA organization representing a specific business function and definite place on the organizational chart under the domain of a manager. Examples of service lines (at VHA) are Homelessness, Primary Care Operations, Emergency Management, Health Informatics, and Quality Standards and Programs
    2. Create additional rows as needed to accommodate all service/business lines that use the CBPs
B. Maximum Tolerable Downtime

1. Determine the Maximum Tolerable Downtime (MTD)[6] for each Service/Business Line. Use the Table B worksheet below to determine MTD for each Service/Business Line. Note: MTD represents the total amount of time leaders/managers are willing to accept for a process outage or disruption
2. MTD is established at the point (e.g. 12 hours, 24 hours, and 30 days) where the potential impact is initially determined to be either moderate or high

Table B-2: MTD Examples
A Service/Business Line using a CBP with high or moderate impact after 24 hours would be assigned an MTD of 24 hours.
A Service/Business Line using a CBP with low impact at 12 hours and high or moderate impact at 72 hours would be assigned an MTD of 72 hours.
A Service/Business Line using a CBP with low impact at 7 days and high or moderate impact at 30 days would be assigned an MTD of 30 days.
A Service/Business Line using a CBP with low impact at >30 days would be assigned an MTD of >30 days.

3. Create additional tables as needed to accommodate all service/business lines that use the CBPs
4. After MTD is determined for each Service/Business Line, transfer the information to Table C, Service/Business Line MTD Summary

[6] When determining MTD, consider the FIPS 199 availability security categorization, which serves as a basis of the BIA

Table B-3: Service/Business Line 1 = *VA human resources and payroll offices* **MTD for Service/Business Line 1 = 12 hours** **(Update OLDE database to reflect the latest personnel changes.)**													
FIPS 199 Availability Impact Rating	**FIPS 199 Potential Impact Definitions/Disruption of access to or use of IS could be expected to have:**	**Point at which adverse effect initially occurs**											
		Immediat	**4 Hours**	**8 Hours**	**12 Hours**	**24 Hours**	**48 Hours**	**72 Hours**	**7 Days**	**14 Days**	**21 Days**	**30 Days**	**> 30 Days**
Low-impact	Limited adverse effect on organizational operations, organizational assets, or individuals.												
Moderate-impact	Serious adverse effect on organizational operations, organizational assets, or individuals.				X								
High-impact	Severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.												
Table B-4: Service/Business Line 2 = *VA human resources and payroll offices, HRIS, and PHRSS* **MTD for Service/Business Line 2 = 12 hours** **(Process personnel actions through PAID (Edit and Update process))**													
FIPS 199 Availability Impact Rating	**FIPS 199 Potential Impact Definitions/Disruption of access to or use of IS could be expected to have:**	**Point at which adverse effect initially occurs**											
		Immediat	**4 Hours**	**8 Hours**	**12 Hours**	**24 Hours**	**48 Hours**	**72 Hours**	**7 Days**	**14 Days**	**21 Days**	**30 Days**	**> 30 Days**
Low-impact	Limited adverse effect on organizational operations, organizational assets, or individuals.												
Moderate-impact	Serious adverse effect on organizational operations, organizational assets, or individuals				X								
High-impact	Severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.												

Table B-5: Service/Business Line 3 = *Financial Service Center (FSC)* **MTD for Service/Business Line 4 = 12 hours** **(Interface personnel data for time reporting in VATAS)**													
FIPS 199 Availability Impact Rating	**FIPS 199 Potential Impact Definitions/Disruption of access to or use of IS could be expected to have:**	**Point at which adverse effect initially occurs**											
		Immediat	**4 Hours**	**8 Hours**	**12 Hours**	**24 Hours**	**48 Hours**	**72 Hours**	**7 Days**	**14 Days**	**21 Days**	**30 Days**	**> 30 Days**
Low-impact	Limited adverse effect on organizational operations, organizational assets, or individuals												
Moderate-impact	Serious adverse effect on organizational operations, organizational assets, or individuals				X								
High-impact	Severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals												

Table B-6: Service / Business Line (that uses CBPs identified in Table B-1)	MTD
Update OLDE database to reflect the latest personnel changes. ***Business Line: VA human resources and payroll offices.***	12 hours
Process personnel actions through PAID (Edit and Update process). ***Business Line: VA human resources and payroll offices, HRIS, and PHRSS.***	12 hours
Interface personnel data for time reporting in VATAS ***Business Line: Financial Service Center (FSC)***	12 hours

Determine Recovery Time Objective and Recovery Point Objective:

1. Enter the Information System name and Recovery Time Objective (RTO)[7] and Recovery Point Objective (RPO)[8]
2. Enterprise Operations (EO) offers three possible DR levels and associated RTOs and RPOs

Table B-7: EO DR Levels, RTO's, and RPO's		
DR Level	**RTO**	**RPO**
Mission Critical	12 hrs	2 hrs
Essential Support	72 hrs	24 hrs
Routine	30 days	24 hrs

3. If the needed infrastructure for the RTO specified in the ISCP and SLA is not yet in place and the system is being recovered under a 30-day RTO until the infrastructure can be completed, enter the RTO as 30 days and RPO as 24 hours

[7] RTO defines the maximum amount of time a system can remain unavailable before there is an unacceptable impact on other systems, supported business processes, and the MTD.

[8] RPO represents the point in time, prior to a disruption or system outage, to which mission/business data can be recovered (given the most recent backup copy of the data) after an outage.

4. Consider work recovery time (WRT), the time it takes for a process or function to become operational after the system is recovered, when determining MTD and RTO. If WRT is needed, RTO should be less than MTD

Table B-8: Information System RTO and RPO		
Personnel and Accounting Integrated Data (PAID)	12 hours	2 hours

Determine Gap (MTD-RTO)

1. List the Service/Business Lines and MTDs from Table C and RTO from Table E
2. The RTO is the same for all Service/Business Lines
3. To determine the gap, subtract the RTO from the MTD for each Service/Business Line. Note: If MTD is less than RTO (MTD – RTO is negative), the issue needs to be addressed

Table B-9: Determine Gap Worksheet			
Service / Business Line (from Table B-3 through Table B-5)	**MTD**	**RTO**	**GAP (MTD – RTO)**
Update OLDE database to reflect the latest personnel changes. Business Line: VA human resources and payroll offices.	12 hours	12 hours	0
Process personnel actions through PAID (Edit and Update). Business Line: VA human resources and payroll offices, HRIS, and PHRSS.	12 hours	12 hours	0
Interface personnel data for time reporting in VATAS Business Line: Financial Service Center (FSC)	12 hours	12 hours	0

Alternate Processing Procedures:

Describe substitute manual processing procedures available that allow the business unit to continue some processing of information that would normally be done by the impacted IS.

Example: Users have access to paper copies of all patient interviews for review & analysis. New interviews are performed on paper in the event that the application is down and entered once it is available again.

Table B-10: Alternate Processing Procedures **(Explanation needed when alternate process are written below)**
There is no alternate process for updating the data in PAID when the application (OLDE/Edit & Update) is unavailable. Alternate processing procedures for payroll processing include: 1. DFAS can be notified to pay everyone a “straight 80” hour pay. 2. Stations could communicate with DFAS to create Remedy tickets to pay new employees.

System Data/Information Owner POC

System Owner	**System Owner Phone/Email**	**System Owner Physical Address**
Representative for System (if applicable)	**Representative for System Phone/Email (if applicable)**	**Representative Physical Address (if applicable)**

BIA Completed by:

APPENDIX C. ACRONYMS

Acronym	Description
ADDM	Discovery and Dependency Mapping
ASD	Architecture, Strategy and Design
BIA	Business Impact Analysis
CBP	Critical Business Process
CMDB	Continuity Management Database
DRP	Disaster Recovery Plan
EDP	Enterprise Design Pattern
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
GRC	Governance Risk and Compliance
ISCP	Information System Contingency Plan
IT	Information Technology
ITSM	Information Technology Service Management
ITWD	Information Technology Workforce Development
MEF	Mission Essential Function
MTD	Maximum Tolerable Down Time
NIST	National Institute of Standards and Technology
OBC	Office of Business Continuity
OLDE database	Online Data Entry Database
OIG	Office of Inspector General

Acronym	Description
OI&T	Office of Information and Technology
OPA	Office of Public and Intergovernmental Affairs
PAID	Personnel and Accounting Integrated Data System
PD	Product Development
PMAS	Project Management Accountability System
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCCM	System Center Configuration Manager
SDE	System Delivery and Engineering
SMART	Security Management and Reporting Tool
SME	Subject Matter Expert
TMS	Talent Management System
TRM	Technical Reference Model
TT&E	Test, Training and Exercise
VA	Department of Veterans Affairs
VATAS	VA Time & Attendance System
VHA	Veterans Health Administration
VIP	Veteran-Centric Integration Process

APPENDIX D. DEFINITIONS

Business Continuity Planning (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes are 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 are 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 GRC-RV (Risk Vision) must be completed and reviewed by required staff (ISOs) prior to either type of visit. If ISOs do not complete this review, issues of completion or response will occur.
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.
NIST SP 800-34	NIST Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, provides instructions, recommendations, and considerations for federal information system contingency planning.
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 briefness 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.
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 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 E: 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	Applicable Reference/ Standard	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 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, *Contingency Planning Guide for Federal Information Systems*	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, *Information System Contingency Planning*	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.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
4	FEMA	Federal Continuity Directive-1, *Federal Executive Branch National Continuity Program and Requirements*	Directive that applies to all Federal organizations to follow when planning their continuity program. It provides direction to the Federal Executive Branch for developing continuity plans and programs.
5	FEMA	Federal Continuity Directive-2, *Federal Executive Branch Mission Essential Functions and Candidate Mission Essential Functions Identification and Submission Process*	This Federal Continuity Directive (FCD) implements the requirements of FCD-1 Annex D, and provides guidance and direction to Federal Executive Branch Departments and Agencies (D/As) to validate and update their Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs).
6	VA	VA Handbook 0320, *VA Comprehensive Emergency Management Program*	This Directive provides Department-wide policy for the development, management and administration of the department of Veterans Affairs Comprehensive Emergency Management Program.
7	VA	VA Handbook 0322, *VA Integrated Operations Center*	This directive assigns emergency preparedness and response responsibilities to all levels of Department management and provides policy for a central point of coordination for these activities within the Department and with other Departments and Agencies.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
8	VA	VA Handbook 0324, *Test, Training, Exercise, and Evaluation Program*	Establishes procedures for the Department of Veterans Affairs (VA) Test, Training, Exercise, and Evaluation (TTE&E) Program

APPENDIX F: INCIDENT MANAGEMENT FORM

Incident Management Form	
Location:	Kansas City VA Medical Center 4801 Linwood Blvd. Kansas City, MO 64128
Disruption Type	Power Outage
Disruption Cause	A storm related power outage with high winds which resulted in tree branches and limbs making contact with power lines.
Assumptions	1. Existing generators malfunctioned and are not an option for backup power. 2. VistA is one system that is down due to the power outage. VistA provides an integrated inpatient and outpatient electronic health record for VA patients, and administrative tools to help VA deliver the best quality medical care to Veterans. 3. After a Major Outage, Kansas City Power and Light Company (KCP&L) Prioritizes: Public safety by restoring power to critical services like hospitals, police and fire stations, and water treatment plants 4. The Kansas City VA Medical Center possesses viable contingency plans that describe procedures for backing up records and/or workarounds until power is restored 5. Manual processing will occur for critical functions until power is restored
Affected System	VistA Imaging System
System Description	The VistA Imaging System houses medical images. These images span a range of specialties, including radiology, pathology, cardiology, wound care, endoscopy, surgery, eye care, dental, nursing, and many others. At VistA Imaging sites, images are typically viewed during rounds, conferences, procedures, consultations, and operations. Workstations are generally located in conference rooms, ICUs, shared ward offices, and clinicians' private offices. Clinicians often review images when placing orders or writing progress notes using VA's Computerized Patient Record System (CPRS). VistA Imaging provides the multimedia component of CPRS, and completes the online CPRS chart by providing ready access to medical images and scanned documents such as signed consent forms, advance directives, and drawings.

APPENDIX G: VISTA IMAGING SYSTEM BUSINESS IMPACT ANALYSIS

VistA Imaging System Business Impact Analysis	
Description	The VistA Imaging System houses medical images. Complete Multi-media Electronic Health Care Record integrates medical images and scanned documents in the patient's chart including patient treatment transcripts and x-rays. Captured images are combined with text data to facilitate a clinician's task of correlating information and making timely and accurate patient care decisions.
System Owner	CIO of the OPA
Critical Business Process	Provide timely and effective patient care
MTD	4 hours, based on the need of the patients to be serviced
RTO	4 hours
MTD-RTO GAP	0 hours
RPO	4 hours
Alternate Procedures	There is no alternate process for retrieving existing patient data. Alternate processing procedures for patient treatment include: Use of a limited number of battery-powered, non-networked laptops for completing patient intake forms, treatment transcripts and prescriptions.