

**VA Enterprise Design Patterns
Information Technology (IT) Service Management**

Business Impact Analysis

**OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)**

**VERSION 1.0
DATE ISSUED: JUNE 2016**



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.marsha
ll@va.gov, cn=Gary E. Marshall 137891
Date: 2016.06.06 13:11:21 -04'00'

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.tibbit
s@va.gov, cn=PAUL A. TIBBITS
116858
Reason: I am approving this document.
Date: 2016.06.06 14:13:09 -04'00'

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

REVISION HISTORY

Version	Date	Approver	Notes
1.0	6/3/2017	Jaqueline Meadows- Stokes	Updated with stakeholder feedback

CONTENTS

1	Introduction	5
1.1	Business Need	6
1.2	Approach	7
2	Current Capabilities and Limitations	7
2.1	Current Capabilities.....	7
2.2	Current Limitations	8
3	Future Capabilities	9
3.1	Utilizing the VA System Inventory (VASI) System or Record (SOR) Process	9
3.2	Determining Which Systems are Vital.....	10
3.3	Recovery/Replacement Measures for Vital Systems	10
3.4	Alignment to the One-VA Technical Reference Model (TRM)	10
3.5	Alignment to Veteran-Focused Integration Process (VIP)	11
4	Use Cases	11
4.1	System-Based BIA.....	11
4.1.1	Overview	11
4.1.2	Assumptions.....	11
4.1.3	Use Case Description	11
4.2	Process-Based BIA	13
4.2.1	Overview	13
4.2.2	Assumptions.....	13
4.2.3	Use Case Description	14
Appendix A.	Scope	16
Appendix B.	Definitions.....	17
Appendix C.	Acronyms	20
Appendix D.	References, Standards, and Policies.....	22
Appendix E.	Seven Steps of the BIA Process From FCD 2	26
Appendix F.	VA Mission Essential Functions Table	27
Appendix G.	Complete BIA Example	28

Table 1: Representative VA ITSM Enterprise Framework Categories and Approved Technologies	10
Table 2: Authority to Operate Technical/Testing Requirements	29
Table 3: Authority to Operate Documentation Requirements.....	30
Table 4: Veteran's Benefits Delivery Network Mission/Processes and System Criticalities	32
Table 5: Veteran's Benefits Delivery Network Time Objectives	33
Table 6: Veterans Benefits Delivery Network Resource Requirements	33
Table 7: Veteran's Benefits Delivery Network Recovery Priorities.....	34
Figure 1: System-Based BIA Flow Chart.....	13
Figure 2: Process Based BIA Process Diagram	15
Figure 3: Process Based BIA Steps	26
Figure 4: List of Primary Essential Functions and Corresponding Offices	27

Figure 5: Veteran's Benefits Delivery Network Mission/Business Processes and Impact Estimated Downtime	32
Figure 6: Veteran's Benefits and Compensation Systems BIA Outputs.....	35

QUICK JUMP

Select an icon to skip to a section.



Current Capabilities



Future Capabilities



Use Cases



One-VA Technical Reference
Model



The Veteran-Focused
Integration Process



Enterprise Design Pattern
Scope

1 INTRODUCTION

The purpose of this Enterprise Design Pattern (EDP) is to provide guidance to Department of Veterans Affairs (VA) projects on how to conduct a Business Impact Analysis (BIA) to support contingency planning, including Continuity of Operations (COOP) and Disaster Recovery Plans (DRP). This guidance will ensure that all projects complete BIAs in a standardized manner to support the completion of risk assessments and the development of contingency plans per VA Directive 6500 policies.

A BIA, as defined by National Institute of Standards and Technology Special Publication (NIST SP) 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, is an analysis of an information system's requirements, functions, and interdependencies. A BIA is required to correlate information systems with critical mission/business processes (e.g., VA's Mission Essential Functions¹ (MEFs)) and respective services. BIA outcomes characterize system contingency requirements, priorities, and the consequences of a disruption. These outcomes inform leadership and system/process owners on investment and recovery strategies for mission critical systems and processes. Additionally, the outcomes provide contingency planning requirements, priorities, backup plans, recovery plans, and Federal Information Security Management Act (FISMA) security controls for all VA System Inventory (VASI) systems

¹ MEFs are a broader set of essential functions that organizations must continue throughout or resume rapidly after a disruption of normal activities.

and non-VASI systems in accordance with Federal Continuity Directive 1 (FCD 1), NIST SP 800-34, Rev. 1 and VA Directive 6500.8 (Appendix D), *Information System Contingency Planning*.

There are two types of BIAs as outlined by Federal Continuity Directive 2 (FCD 2) and NIST SP 800-34, Rev. 1: 1) process-based and 2) system-based. A process-based BIA utilizes a risk management, function-centric methodology to ensure that MEFs are appropriate and relevant to the assigned federal agency.

The key steps in accomplishing a BIA, as described in the following sections, include:

- Determining mission/business process and recovery criticality
- Identifying resource requirements
- Identifying recovery priorities for system resources

A process-based BIA determines level of risk, recovery time requirements and objectives, vulnerability values, and required mitigation strategies for continued MEF support. Outcomes from a process-based BIA will aid in the development of Continuity of Operations (COOP) plans for the continuation of essential functions. A system-based BIA correlates systems with critical mission/business processes and serves to characterize the consequences of a disruption to those systems. Currently, per VA Directive 6500.8, Information System Contingency Planning, all systems listed in the VA Systems Inventory Systems of Record (VASI SOR) are required to conduct a system-based BIA prior to obtaining an Authority to Operate (ATO). It will determine the mission and business processes supported by the system, the recovery criticality² of the system including impact level and time metrics, and recovery investment requirements for the system.

1.1 Business Need

A BIA validates the VA Primary Mission Essential Function (PMEF) to “provide medical and hospital services for Veterans, and during a disaster or emergency, for civilian victims as appropriate,” and validates VA’s MEFs so they continue despite a disruption of normal activities or resume rapidly thereafter. Additionally, a BIA informs contingency planning efforts that directly address a material weakness identified by VA Office of Inspector General (OIG) during its fiscal year (FY) 2015 FISMA audit (Finding 5, Recommendation 24), as referenced in Appendix D.

A standardized approach to an enterprise BIA is required to adequately assess, identify, and prepare for the impact of a disruption to mission critical systems, vital business processes, or

² Recovery criticality includes impact of a system disruption, outage impacts, and estimated downtime. Downtime should reflect the maximum that an organization can tolerate while maintaining the mission.

MEFs. A process-based BIA will help determine which processes are mission critical. Conversely, a system-based BIA will help determine which systems require more planning, preparation, support, investments, and recovery strategies. A BIA will also support consistency across other contingency planning artifacts such as COOP, Business Continuity Planning (BCP), and DRP.

1.2 Approach

VA's near term approach leverages existing BIA enterprise processes to:

- Evaluate current information technology (IT) systems and critical business processes within the different VA business lines and identify the individual baseline process that involve the BIA
- Identify gaps between the baseline process, services, and mission-critical IT systems for BIA and VA/Federal guidance
- Engage internal stakeholders to bridge process gaps for an enterprise BIA
- Identify process improvements based on vendor inputs and feedback to identify industry best practices for leveraging BIA

A standardized approach to conducting a BIA in VA will:

- Help VA identify and evaluate the impact of disasters to provide the basis for investment in recovery strategies
- Assist in developing prevention and mitigation strategies, and prioritizing critical systems and functions from an enterprise perspective
- Support consistent development of COOP, BCP, and DRP to obtain ATOs



2 CURRENT CAPABILITIES AND LIMITATIONS

The following subsections describe current BIA capabilities leading to recommendations for standardized BIAs for future IT system deployments. Understanding the current BIA process and how it is utilized within VA will identify gaps between the current capabilities and the future enterprise-level BIA.

2.1 Current Capabilities

The Office of Business Continuity (OBC) is responsible for managing the BIA process within VA and facilitating BIA completion for each system owner. The process involves coordination between OBC, system owners and business partners to identify mission-critical systems and processes utilizing a BIA. The BIA incorporates results into the strategy development efforts for the organization's COOP and DRP programs.

The BIA supports all activities for obtaining an ATO in VA information systems. The Governance, Risk, and Compliance (GRC) tool, RiskVision, is the central repository for all systems within VA that meet the requirements for receiving an ATO. Some elements of the BIA process are located within the VASI, a precursor to an ATO.

VA policies and guidance documents (e.g., VA Directive 6500, Information Security Program and VA Handbook 6500.8, Information System Contingency Planning) establish operational requirements and provide specific procedures for IT Contingency Planning. The VA Handbook aligns to contingency planning controls located in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST SP 800-34, Rev. 1 provides the steps for performing and accomplishing a BIA during the System Development Lifecycle (SDLC). These guidance documents validate the importance of a BIA and offer a framework for developing a new BIA or for strengthening existing processes.

An Information Security Contingency Planning (ISCP) template designed for system owners and restricted personnel analyze systems to determine their importance. Individual systems within the enterprise each require tailored ISCP templates. The ISCP template includes a BIA template as an appendix.

2.2 Current Limitations

The VA approach to BIA at the enterprise level is inconsistent for all FISMA required systems. This has resulted in a lack of adequate assessment of many of these systems and the creation of independent processes for analyzing risk and impact. Four key challenges limit implementation of a successful, VA-wide enterprise BIA process. They are:

- **Resources:** The OBC owns the BIA process and is responsible for ensuring the completion of BIAs in VA, including on systems within the GRC repository scheduled for ATO. Limited resources make it difficult for OBC to ensure consistent, enterprise wide the BIA process alignment.
- **Training:** System owners lack adequate training on how to conduct an appropriate system-based BIA and are unaware of the tools and process for completion and submission of the BIA. Additionally, system owners lack understanding of the BIA questions and therefore have difficulty responding appropriately.
- **Process:** The ISCP BIA template provides guidance on how to perform a BIA but involves a manual process for completion and submission that leads to exhaustion of current resources for oversight.
- **Legislation:** Policies that outline the requirements for a BIA exist, but there is no reference in the Office of Information Security (OIS) Authorization Requirements

Standard Operating Procedures (SOP) that mandates accountability and forces business lines to complete the BIA. Without a mandate, VA systems can receive an ATO without completing a BIA.



3 FUTURE CAPABILITIES

Utilizing a standardized, enterprise-level BIA process based on the 7-step process outlined in Appendix E will ensure that VA has a consistent approach to information system contingency planning, including evaluating and planning for the potential effects of an interruption to systems that support VA's PMEF resulting from a disaster or emergency as well as meeting requirements outlined by FISMA. The standardized BIA process will validate identification of vital systems, and assures system availability during a disruption so that mission critical processes and services resume quickly and perform as required. The following future capabilities will ensure that VA is equipped to analyze risk, determine the impact, and provide recovery and alternate solutions:

- Having adequate oversight resources to support the BIA process and ensure proper FISMA security controls regarding impact and vulnerability are assigned
- Utilizing the appropriate FISMA system classification levels based on criticality and impact to the organization
- Employing an automated system or tool that interfaces with applicable VA systems to streamline the BIA process given project and organizational resource constraints
- Leveraging templates in the NIST guidelines and FCD 2 will be used for the system/processed based BIAs
- Conducting training classes to increase stakeholder awareness of the need to utilize the BIA process and how to populate and submit a completed BIA
- Creating a standard operating procedures designed to provide a step-by-step corresponding guidance document for when system owners conduct the BIA interviews to help provide clarification of the BIA questions and their importance
- Establishing and enforcing an enterprise-wide policy that will increase accountability for completing the BIA within VA
- Implementing a governance process to ensure adherence to the BIA process

3.1 Utilizing the VA System Inventory (VASI) System or Record (SOR) Process

The VASI is the authoritative data source for VA IT systems and is a vital component of the Department's Enterprise Architecture. This SOR is a department-wide inventory of systems and systems-related information, and provides the current state of VA's IT environment. Risk management analysis validates these systems before the system's inclusion in the VASI SOR and

it receives an ATO. This validation process provides a departmental process for conducting both risk management and BIA.

3.2 Determining Which Systems are Vital

All mission-critical systems directly support one of VA's MEFs. Therefore, all resources deemed "vital" require a BIA. This includes IT systems that support Veteran's and clinicians, and systems, devices, and processes which aid communication in the event of a disaster. Systems that aid in identifying and treating patients under Veterans Health Administration's (VHA) direct care are also required to complete a BIA.

3.3 Recovery/Replacement Measures for Vital Systems

The success of vital systems depends on its ability to continue during an emergency, rapidly recover after failing, or the ability to transfer that system's function to another system. An analysis of the likelihood of failure, recovery options, and/or replacement options is paramount to the success of establishing a functional and proactive BIA. System owners ensure that the RiskVision tool includes the results of the BIA as part of the development of required contingency planning artifacts.



3.4 Alignment to the One-VA Technical Reference Model (TRM)

The VA Technical Reference Model (One-VA TRM) establishes a common vocabulary and structure for describing the IT used to develop, operate, and maintain enterprise applications.

All projects that deploy systems based on the BIA are required to use the approved tools and technologies located in the TRM. Table 1 includes relevant tools.

TABLE 1: REPRESENTATIVE VA ITSM ENTERPRISE FRAMEWORK CATEGORIES AND APPROVED TECHNOLOGIES

Tool Category	Example Approved Technologies
Configuration Management Database (CMDB)	CA Service Desk Manager, BMC Remedy, Legacy CMDBs
Endpoint Manager	IBM Endpoint, Microsoft SCCM
Patch Management	IBM Endpoint, Microsoft SCCM
Asset Management	CA IT Asset Manager
Relationship and Dependency Mapping	BMC ADDM, CA Configuration Automation
Line of Business	VA System Inventory
Configuration Change Control	CA Configuration Automation
Data Normalization	BMC ADDM, CA IT Asset Manager (SAM)



Scanning and Discovery	Nessus, IBM Endpoint, Microsoft SCCM, CA Configuration Automation
------------------------	---

3.5 Alignment to Veteran-Focused Integration Process (VIP)

VIP is a Lean-Agile IT delivery and oversight framework that services the interest of Veterans through the efficient, secure and predictable streamlining of activities that occur within VA. All projects subject to VIP require an ATO prior to Critical Decision 2 using the assessment and authorization (A&A) process in ProPath. Evaluations of security controls based on an understanding of business needs and mission criticality, supported by the BIA process, drive the ATO. A BIA supports contingency planning artifact requirements for obtaining an initial ATO or renewal of a current ATO for identified critical systems in VA.



4 USE CASES

The following use cases are examples that demonstrate the application of the capabilities and recommendations described in this document.

4.1 System-Based BIA

4.1.1 Overview

The Veterans Benefits Administration (VBA) is implementing a new database and payment system for all education benefit programs. VBA employees will use the system to determine eligibility for benefits as well as processing benefit payment transactions. In order to obtain an ATO, the system must complete a BIA to support the development of a DRP. The system-based BIA will 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.

4.1.2 Assumptions

System owners are responsible for completion and submission of the completed BIA

4.1.3 Use Case Description

The following are steps initiating and completing the BIA:

- **Step 1: Collaborate with OBC:** Reach out to OBC for guidance on completing a BIA, confirm use of the BIA template in NIST Special Publication 800-34 Rev. 1 (Contingency Planning Guide for Federal Information Systems).

- **Step 2: Identify Stakeholder/System Owners:** Determine relevant users, managers, mission/business process owners, and other internal or external points of contact (POC) who will be involved in completing the BIA. The selected individuals should have a strong understanding of VA environment and systems to respond to the questions in the template.
- **Step 3: Train Stakeholders:** Coordinate with OBC to schedule training for identified stakeholders/system owners to discuss completing the BIA.
- **Step 4: Complete BIA:** For example BIA template data, see Appendix G.
 - **4a Determine Process and System Criticality:** Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.
 - **4b Identify Outage Impacts**
 - Identify types of impacts that a system disruption is likely to create
 - Determine values for assessing levels of severity for each impact
 - Assign values for each impact category for each mission/business process
 - **4c Estimate Downtime**
 - Determine Maximum Tolerable Downtime (MTD): total amount of time that is acceptable for a mission/business process outage or disruption
 - Determine Recovery Time Objective (RTO) – maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes
 - Determine Recovery Point Objective (RPO) – Point-in-time, prior to a disruption or system outages to which mission/business process data must be recovered
 - For each mission/Business Process, assign MTD, RTO, and RPO values
 - **4d Identify Resource Requirements**
 - Identify system resources, including hardware, software, and data files
 - **4e. Identify Recovery Priorities for System Resources**
 - Determine order of recovery for system resources along with expected time for recovering the resource following a disruption that requires a complete rebuild, repair, or replacement
- **Step 5: Prepare Findings:** Once completed, OBC submits, reviews, and validates the results of the BIA. After validation, prepare a formal report to share with any necessary stakeholders. This report includes at a minimum the business functions, the criticality and impact assessments and the maximum tolerable downtime (MTD) assessment. It should also include initial impact findings and issues to be resolved.

- **Step 6: Submit Findings:** The results of the BIA are included in the package submitted for the ATO. The BIA analysis and findings serve to build various system recovery policies focused around DRP policies.

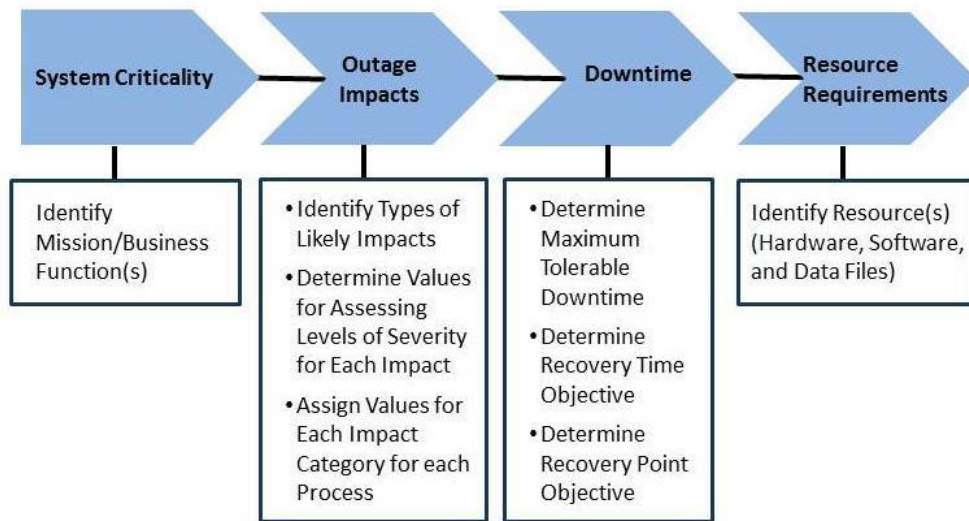


FIGURE 1: SYSTEM-BASED BIA FLOW CHART

4.2 Process-Based BIA

4.2.1 Overview

The VHA Office of Emergency Management (OEM) is responsible for analyzing the risk level of the VA PMEF to understand the potential impact to Veterans if a natural, technological, or human caused disaster disrupted these essential functions.³ To accomplish this effort, the VHA OEM is conducting a preliminary BIA on the VA PMEF. The VA PMEF focuses on offering Veterans high-quality health care from doctors and nurses. VHA offers tools and information to help Veterans reach optimal health. The BIA will identify the level of impact on its functions during a disruption. The results from the completed BIA will identify the consequences of a disruption or degradation to the PMEF. These risks can then be mitigated against, planned for, and detailed in applicable policies.

4.2.2 Assumptions

- VA has identified all of their PMEF and MEF systems
- Risk levels have been established for each PMEF
- PMEF has existing continuity of operations plans for critical mission systems

³ Threat and Hazard Identification and Risk Assessment Guide-CPG 201, August 2013

4.2.3 Use Case Description

The following are necessary steps for initiating the BIA process:

- **Step 1:** Identify Stakeholder/System Owners: The VHA OEM ISO collaborates with VHA business partners and the OBC to identify key stakeholders and system owners within their offices responsible for the completion of the BIA. The selected individuals should have a strong understanding of the VA environment and PMEFs in order to properly respond to the questions in the template
- **Step 2:** Collaborate with OBC: The identified system owners reach out to OBC to receive access to the PMEF BIA Worksheet and obtain training, if needed.
- **Step 3:** Complete BIA PMEF Worksheet: The stakeholders/system owners interview the business owners and use the data to complete the BIA spreadsheet. Steps towards the completion of the BIA include completing the following sections of the worksheet. An example of the BIA PMEF Worksheet and section descriptions (high-level details provided below) can be found in the FCD 2 document.⁴
 - **3a** Identify the potential threat or hazard to be considered when determining the impact on PMEF
 - **3b** Describe the vulnerability and potential point of failure of the PMEF to the identified threat or hazard
 - **3c** Determine the vulnerability value for a PMEF in the event of the identified crisis/hazard situation or emergency. This step determines the level of vulnerability of the disruption to this function (e.g., rated at 10 – Critically High –is grave vulnerability to mission performance)
 - **3d** Describe the likelihood of the identified threat or hazard occurring.
 - **3e** Determine the likelihood of the identified crisis/hazard situation or emergency.
 - **3f** Describe the impact to the PMEF by the identified threat or hazard.
 - **3g** Determine the impact of the failure of the identified PMEF in the event of the crisis/hazard situations or emergency.
 - **3h** Estimate the potential downtime as a result of the identified threat or hazard
 - **3i** Define the mandated recovery time for the PMEF support. (e.g., 48 hours to ensure there is not a large gap in patient care)
 - **3j** Determine the risk assessment value through the summation of the vulnerability, the likelihood, and the impact of the Threat or Hazard on a PMEF. The worksheet automatically sums the value.

⁴ <http://www.fema.gov/media-library-data/1386609058811-b084a7230663249ab1d6da4b6472e691/FCD2-Signed-July-2013.pdf>

- **3k** Determine the impact of the PMEF downtime and/or failure.
- **Step 4: Prepare Findings:** Once completed, OBC receives, reviews, and validates the results of the BIA. After validation, the VHA OEM ISO prepares a formal report to share with any necessary stakeholders. This report includes at a minimum the business functions, the criticality and impact assessments and the maximum tolerable downtime (MTD) assessment for the VHA PMEF. It should also include initial impact findings and issues to be resolved.
- **Step 5: Design Risk Mitigation Strategies:** In the event of PMEF service disruption, BIA findings shape understanding of the level of risks and mitigation strategies necessary to continue operations. The BIA analysis and findings also serve to build various business continuity policies focused around COOP policies



FIGURE 2: PROCESS BASED BIA PROCESS DIAGRAM



APPENDIX A. SCOPE

Scope

A BIA identifies and prioritizes information systems and components critical to supporting the organization's mission/business processes. Each VA system should be subject to a BIA. This Enterprise Design Pattern makes recommendations for an enterprise wide BIA that documents the potential impact resulting from scheduled and unscheduled changes and associated processes.

Intended Audience

This document is intended for use by all project-level integrated product teams (IPTs) that are deploying IT systems in an official VA production environment. Each system requires a BIA to determine appropriate backup and recovery plans, and FISMA security controls consistent with NIST SP 800-53 and the VA 6500 Handbook. The output of the BIA supports planning for ATO prior to the system's deployment in the production environment. The production environment consists of both on-premises data centers and externally managed service providers.

Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from Office of Information Technology (OI&T), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Veterans Health Administration (VHA), Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA) provided extensive input and participation. Development of the document included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Approved List	A list of discrete entities, such as hosts or applications, known to be benign and are approved for use within an organization and/or information system.
Authentication (FIPS 200)	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authority to Operate	A formal declaration by a designated approving authority that authorizes operation of a product or system and explicitly accepts the risk to agency operations
Business Impact Analysis	Identifies and prioritizes information systems and components critical to supporting the organization's mission/business processes
Benefits Delivery Network	A suite of COBOL mainframe applications that collectively make up VA's primary claims processing, tracking and payment system
Enterprise Architecture	The description of an enterprise's entire set of information systems, explaining system: configuration, integration, external environment interfaces at the enterprise's boundary, enterprise mission operations support, and the system's contribution to the enterprise's overall security posture.
Governance Risk and Compliance	The central repository for all systems within VA which meet the requirements for receiving an ATO
Information Security Contingency Planning Assessment Template	Designed for system owners and restricted personnel to use when analyzing systems to determine if those systems are critical. It can be tailored for individual systems within the enterprise
Information System User (CNSSI-4009)	Individual or (system) process acting on behalf of an individual, authorized to access an information system.

Key Term	Definition
Information Technology (40 U.S.C., Sec. 1401)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. Equipment is used by an executive agency if the equipment is directly used by the executive agency or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment, in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Maximum Tolerable Downtime (MTD)	The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail required when developing recovery procedures, including their scope and content.
Primary Mission Essential Function	To provide medical and hospital services for Veterans, and during a disaster or emergency, for civilian victims as appropriate.
Recovery Point Objective (RPO)	The RPO represents the point in time, prior to a disruption or system outage, in which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.
Recovery Time Objective	RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.
Remediation	The act of correcting vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application.

Key Term	Definition
Risk	The probability that a particular threat will exploit a particular vulnerability.
System	A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operation environment. When not used in this formal sense, the term is synonymous with the term "host". The context of the word determines the definition, or the definition is specified.
System Owner	Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system.
Threat	Any circumstance or event, deliberate or unintentional, with the potential for causing harm to a system.
User	See "Information System User"
VASI	VASI is 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.
VA Technical Reference Model	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
Veteran-focused Integration Process (VIP)	A Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation, which a threat device could trigger or exploit.

APPENDIX C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
ATO	Authority to Operate
BIA	Business Impact Analysis
BCP	Business Continuity Plan
BDN	Benefits Delivery Network
COOP	Continuity of Operation
COTS	Commercial Off-the-shelf
DHS	Department of Homeland Security
DRP	Disaster Recovery Plan
EO	Enterprise Operations
ESE	Enterprise Systems Engineering
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GRC	Governance, Risk and Compliance
IRP	Incident Response Plan
ISO	Information System
ISCP	Information Security Contingency Planning
MEF	Mission Essential Function
ATO	Authority to Operate
BIA	Business Impact Analysis
BCP	Business Continuity Plan
BDN	Benefits Delivery Network
COOP	Continuity of Operation
COTS	Commercial Off-the-shelf
DHS	Department of Homeland Security
DRP	Disaster Recovery Plan
EO	Enterprise Operations
ESE	Enterprise Systems Engineering
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GRC	Governance, Risk and Compliance
IRP	Incident Response Plan
ISO	Information System
ISCP	Information Security Contingency Planning
MEF	Mission Essential Function
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology

Acronym	Description
OBC	Office of Business Continuity
OI&T	Office of Information and Technology
OIS	Office of Information Security
PMEF	Primary Mission Essential Function
RA	Risk Assessment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDE	System Design Engineering
SDLC	System Development Lifecycle
SSP	System Security Plan
TRM	Technical Reference Model
TS	Office of Technology Strategies
VA	Department of Veterans Affairs
VASI	Veterans Affairs Systems Inventory
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VIP	Veteran-focused Integration Process

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP 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 Enterprise Technical Architecture (ETA):

#	Issuing Agency	Policy, Directive, or Procedure	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	VA	VA Directive 0320: VA Comprehensive Emergency Management Program	This Directive addresses emergency management policies regarding planning, mitigation, response and recovery, including the continuation and rapid restoration of the Department's vital functions under all conditions.
3	VA	VA Directive 0322: VA Integrated Operations Center	The Directive provides VA policy and responsibilities for the VA Integrated Operations Center.
4	VA	VA Directive 0324: Test, Training, Exercise, and Evaluation Program	This Directive establishes Department-wide policy and responsibilities for VA Test, Training, Exercise, and Evaluation Program, in accordance with National Security Presidential Directive 51/Homeland Security Presidential Directive 20, Presidential Policy Directive 8, and the National Preparedness Goal's established interagency exercise and evaluation guidance under the National Exercise Program.
5	VA	VA Directive 6500: Managing Information Security Risk-VA Information Security Program	This directive provides the framework for VA's Security Risk Management Program. VA Handbook 6500 and other VA security handbooks provide additional information, procedures/processes, and roles and responsibilities for achieving the goals and steps outlined in the Directive.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
6	DOD	National Security Presidential Directive 51 / Homeland Security Presidential Directive 20	This policy establishes “National Essential Functions,” prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.
7	DHS	Federal Continuity Directive 1	This directive provides direction to the Federal Executive Branch for developing continuity plans and programs. Continuity planning facilitates the performance of executive branch essential functions during all-hazards emergencies or other situations that may disrupt normal operations. The ultimate goal of continuity in the executive branch is the continuation of National Essential Functions.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
8	DHS	Federal Continuity Directive 2	This directive 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 and Primary Mission Essential Functions. It includes guidance and checklists to assist agencies in assessing their essential functions through a risk management process and in identifying candidate PMEfs that support the National Essential Functions. The most critical functions necessary to lead and sustain the Nation during a catastrophic emergency. This FCD provides direction on the formalized process for submission of D/As candidate PMEfs in support of the NEFs. This FCD also includes guidance for conducting a Business Process Analysis (BPA) and Business Impact Analysis (BIA) for MEFs and candidate PMEfs. Process and impact analysis identify essential function relationships, interdependencies, time sensitivities, threats and vulnerabilities, and mitigation strategies that impact and support the performance of the MEFs and PMEfs.
9	NIST	NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems	This publication provides instructions, recommendations, and considerations for federal information system contingency planning.
10	VA	VA Handbook 6500.8: Information System Contingency Planning	To establish operational requirements and provide specific procedures for the implementation of Information System Contingency Planning as required by VA Directive and Handbook 6500, Information Security Program, dated August 4, 2006 and September 18, 2007, respectively.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
11	VA	VA Directive 6404: VA Systems Inventory	This directive establishes the Department of Veteran Affairs (VA) Systems Inventory (VASI) as the authoritative source for VA Information Technology (IT) Systems and defines the objectives, principles, roles and responsibilities for the utilization, management and sustainment of the VA Systems Inventory.
12	VA	OIG FISMA Audit FY15	Recommendation 24 for Finding 5 (Contingency Planning): “We recommended the Assistant Secretary for Information and Technology perform and document a Business Impact Analysis for all systems and incorporate the results into an overall strategy development effort for contingency planning. (This is a new recommendation.) “

APPENDIX E. SEVEN STEPS OF THE BIA PROCESS FROM FCD 2

The BIA referenced here is a COOP process focused BIA which is inherent to FCD 2 ensuring that MEFs are able to be continued during all hazards and all threats. The Process consists of seven steps, as outlined below. There is a system specific BIA outlined in NIST 800-34, rev. 1 which focuses on identifying critical mission/business systems. The system based BIA does not include the steps below.

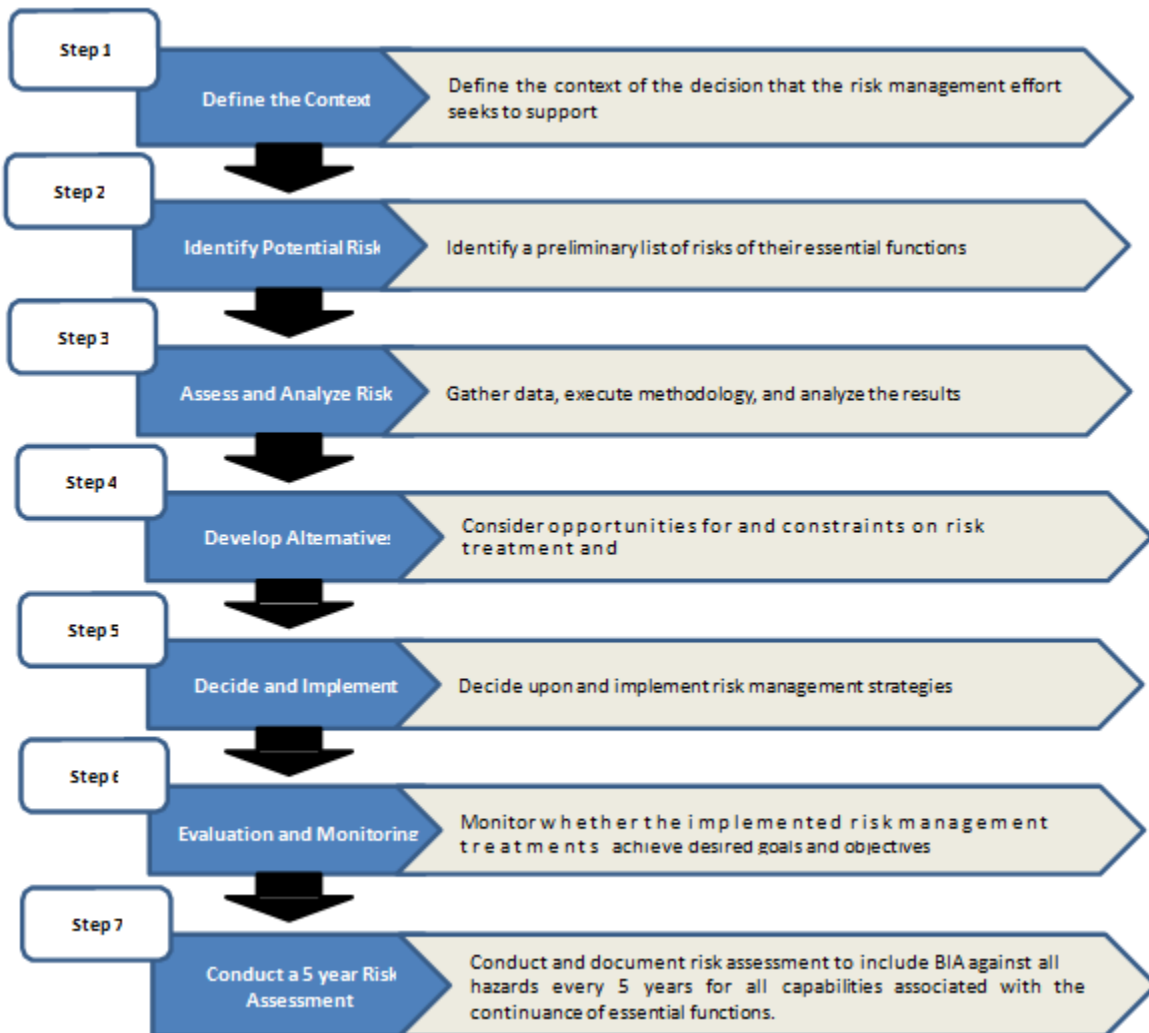


FIGURE 3: PROCESS BASED BIA STEPS

APPENDIX F. VA MISSION ESSENTIAL FUNCTIONS TABLE

Figure 4, below, lists functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base. The lack of the continuation of these MEFs could result in severe consequence include loss of life, vital resources, and security. A BIA identifies the consequences of disruptions to these functions and processes and gathers information required to develop recovery strategies for both BCPs and DRPs.

VA PMEF: Provide medical and hospital services for Veterans, and during a disaster or emergency, for civilian victims as appropriate.	
VA MEF	Responsible Office
Healthcare to Veterans	Veterans Health Administration
VA/DoD Contingency System	Veterans Health Administration
Furnish VA hospital care to responders and victims	Veterans Health Administration
National Disaster Medical System (NDMS)	Veterans Health Administration
Process insurance	Veterans Benefits Administration
Pay Veterans and beneficiaries	Veterans Benefits Administration
Veteran burial services	National Cemetery Administration
Support to National Response Framework (NRF)	Office of Operations, Security, & Preparedness
Account for employees	Office of Human Resources and Administration
Maintain communication capabilities related to MEFs/PMEF	Office of Information and Technology
Ensure payment capabilities	Office of Management
Acquisitions support	Office of Acquisitions, Logistics, & Construction

FIGURE 4: LIST OF PRIMARY ESSENTIAL FUNCTIONS AND CORRESPONDING OFFICES

APPENDIX G. COMPLETE BIA EXAMPLE

VETERANS BENEFITS ANALYSIS BENEFITS AND COMPENSATION SYSTEMS BIA OVERVIEW

The Veterans Benefits Administration (VBA) is planning to release a new set of systems that provide claims processing, training, and outreach for Veteran benefits and compensation into the VA IT enterprise. Results from a BIA will determine which of these systems are mission-critical priorities. Each system will be assessed for testing/technical requirements and documentation requirements, including an Information Security Contingency Planning Assessment. Once complete, security/recovery strategies can be developed to determine investment thresholds, recovery solutions, and system alternatives.

ASSUMPTIONS

- All systems and system owners are maintained and regulated by VA
- Prioritization levels are predetermined

DESCRIPTION

A recent review of the existing benefits system within VBA validated a need to create a set of benefits and compensation systems for claims processing, training, and outreach. The three selected systems that provide claims processing, training, and outreach for Veteran benefits and compensation are:

- **Benefits Delivery Network (BDN)** - Tracks and distributes approximately \$40 Billion in Veteran entitlements yearly. BDN is the primary database and payment system for all education benefit programs administered by Education Service. VBA employees use BDN for the purpose of determining eligibility for benefits as well as processing benefit payment transactions. BDN processes claims for all education benefits.
- **Benefits Assistance Service (BAS) Outreach Reporting Tool** - A robust outreach tool that captures Personally Identifiable Information (PII), demographic data, and claim data is needed to properly report to leadership and Congress on VBA's outreach efforts.
- **Compensation and Pension Training** - A family of Computer Based Training (CBT) programs that combine interactive CBT and electronic support with small group cooperative learning events

Each system must go through an extensive assessment in order to gain an ATO. This includes the following Technical/Testing Requirements and Documentation Requirements outlined in Tables 2 and 3.

TABLE 2: AUTHORITY TO OPERATE TECHNICAL/TESTING REQUIREMENTS

Baseline Platform Image	<ul style="list-style-type: none"> • For each host, there must be an approved baseline platform (operating system, database, etc.) image installed • Platforms should be limited to one baseline build; any exceptions must be documented and approved • All baseline image builds must be configured using approved hardening guidance for operating systems, databases, and network devices • Baseline image must be managed through the Change Management process with changes approved through a Change Control Board
Nmap Scan	<ul style="list-style-type: none"> • A network discovery scan must be conducted to include all IP addresses within the system boundary mapped back to specific components within the system architecture
Tenable Nessus Scan	<ul style="list-style-type: none"> • A vulnerability scan against all instantiations of the operating system must be conducted to identify security flaws • Actual scan results must be provided for analysis • All vulnerability scans that identify Critical and/or High findings will be remediated or have a documented mitigation plan
HP Fortify Static Code Analyzer	<ul style="list-style-type: none"> • A Fortify Static Code Analyzer must be conducted to identify security vulnerabilities, coding, and design flaws within applications • All terminal findings (e.g., STIG Cat I/II, Fortify Critical/High, OWASP) must be remediated
Security Configuration Compliance Scan	<ul style="list-style-type: none"> • Compliance scans must check against approved hardening guidance for operating systems, databases, and network devices • A compliance scan using an SCAP validated scanning tool must be conducted with a passing result (> 80% compliant)
Application Assessment / Pen Test	<ul style="list-style-type: none"> • Full application assessment or penetration test must be performed that includes automated & manual assessment tools and techniques • An IBM App Scan should be performed against all web applications to identify security vulnerabilities

TABLE 3: AUTHORITY TO OPERATE DOCUMENTATION REQUIREMENTS

System Security Plan (SSP)	<ul style="list-style-type: none"> • The SSP must include a network diagram and confirmation of the security accreditation boundary that includes all devices and supporting software architecture • The SSP will be generated through the Agilance RiskVision Open GRC tool
Risk Assessment (RA)	<ul style="list-style-type: none"> • The RA will be generated through the Agilance RiskVision OpenGRC tool • Guidance is found in NIST SP 800-30
Configuration Management Plan (CMP)	<ul style="list-style-type: none"> • The CMP should include infrastructure devices and baseline configurations (e.g., switches, routers, firewalls) • The CMP should include a configuration file for each operating system(s), database(s), application(s), and network device(s) to validate compliance with baseline configuration
Incident Response Plan (IRP)	<ul style="list-style-type: none"> • VA-Network Security Operations Center (VA-NSOC is responsible for National level tasks associated with incident response • Each site is responsible for developing local level procedures incorporating VA-NSOC areas or responsibility
Signatory Authority	<ul style="list-style-type: none"> • All package submissions must include this document signed and dated by the appropriate parties
Information Security Contingency Plan (ISCP)	<ul style="list-style-type: none"> • ISCP consolidates the results of a BIA with those of a threat and vulnerabilities assessment to facilitate the preparation of information technology contingency plans and the related training, testing, and exercises • Includes data backup procedures, recovery procedures, data and functionality validation testing, concurrent processing, and a BIA

A part of the ATO for Veterans benefits and compensation includes a BIA, which will identify and prioritize system components by correlating them to the mission / business processes the system supports, and use this information to characterize the impact on the processes if the system were unavailable. See below for a sample BIA.

Business Impact Analysis for the Veteran's Benefits Delivery Network

Overview: This BIA is part of the contingency planning process for the BDN. It was prepared on April 30, 2016.

Purpose: The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business processes the system supports, and to use this information to characterize the impact on the processes, if the system is unavailable.

The BIA is composed of the following three steps:

1. **Determine 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 time an organization tolerates 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 identified 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, clearly link system resources to critical mission/business processes. Establish priority levels for sequencing recovery activities and resources.

This document is used to build the BDN ISCP and is a key component of the ISCP. It also may be used to support the development of other contingency plans associated with the system, including, but not limited to, the DRP or Cyber Incident Response Plan (CIRP).

System Description: The BDN is a suite of common business oriented language (COBOL) mainframe applications that collectively make up the VA's primary claims processing, tracking, and payment system.

BIA Data Collection:

Table 4, below, summarizes the impact on each mission/business process if BDN were unavailable, based on the following criteria:

- Financial Impact
- Personnel Impact
- Business Process Impact
- Regulatory Impact

TABLE 4: VETERAN'S BENEFITS DELIVERY NETWORK MISSION/PROCESSES AND SYSTEM CRITICALITIES

Mission/Business Process	Description
Veterans claims processing, tracking, and payment system.	Process of tracking and distributing veteran entitlements
Primary database and payment system for education benefits programs	Database that houses all education benefit programs administered by Education Service.
Determine eligibility for benefits	VBA employees use BDN for the purpose of determining eligibility for benefits
Processes benefit payment transactions and education claims	VBA employees use BDN for the purpose of processing benefit payment transactions and claims for Education benefits

BDN Mission/Business Processes and Associated Impact					
Mission/Business Process	Impact Category				
	Financial Impact	Personnel Impact	Business Process	Regulatory Impact	Impact
Veterans claims processing, tracking and payment system	5	2	4	2	<i>Moderate (13)</i>
Primary database and payment system for education benefits programs	7	3	3	2	<i>Moderate (15)</i>
Determine eligibility for benefits	6	2	2	0	<i>Minimal (10)</i>
Processes benefit payment transactions and education claims	10	3	2	5	<i>Severe (20)</i>

FIGURE 5: VETERAN'S BENEFITS DELIVERY NETWORK MISSION/BUSINESS PROCESSES AND IMPACT ESTIMATED DOWNTIME

Below identifies the MTD, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on BDN. Values for MTDs and RPOs are expected to be specific periods, identified in hourly increments (i.e., 8 hours, 36 hours, 97 hours, etc.). The time objectives include:

- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or

disruption and includes all impact considerations. Determining MTD is important because MTD provides continuity planners with precise direction on (1) the selection of an appropriate recovery method, and (2) the depth of detail required to develop recovery procedures, including their scope and content.

- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.
- **Recovery Point Objective (RPO).** The RPO represents the point in time, prior to a disruption or system outage, at which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

TABLE 5: VETERAN'S BENEFITS DELIVERY NETWORK TIME OBJECTIVES

Mission/Business Process	MTD	RTO	RPO
Veterans claims processing, tracking and payment system	<i>72 hours</i>	<i>48 hours</i>	<i>12 hours (last backup)</i>
Primary database and payment system for education benefits programs	<i>48 hours</i>	<i>24 hours</i>	<i>12 hours (last backup)</i>
Determine eligibility for benefits	<i>97 hours</i>	<i>72 hours</i>	<i>32 hours (last backup)</i>
Processes benefit payment transactions and education claims	<i>24 hours</i>	<i>12 hours</i>	<i>8 hours (last backup)</i>

Resource Requirements:

Below identifies the resources that compose *BDN* including hardware, software, and other resources such as data files.

TABLE 6: VETERANS BENEFITS DELIVERY NETWORK RESOURCE REQUIREMENTS

System Resource/Component	Platform/OS/Version (as applicable)	Description
BDN Web Site	Website	To give VA employees access to BDN/Beneficiary Identification Records

Benefits Delivery Network - Education Systems Web Apps	Application	Suite of applications within the BDN that support providing educational benefits to military service members, Veterans, and their spouses/dependents
Benefits Delivery Network - Payment History Web App	Application	Payment History File that allows retrieval of payment and returned payment info for all the benefit systems that are paid through BDN and VETSNET
Benefits Delivery Network - Web Reports Site	Website	Cost effective replacement vehicle for BDN hardcopy printing and distribution of BDN statistical reports to the VACO, RPO, and RO community
Benefits Delivery Network - Education Systems Web Apps	Application	Suite of applications within the BDN that support providing educational benefits to military service members, Veterans, and their spouses/dependents

Order of Recovery:

Table 8 below lists the order of recovery for BDN resources. The table also identifies the expected time for recovering the resource following a “worst case” (complete rebuild/repair or replacement) disruption. The table outlines the Recovery Time Objective (RTO) for each system resource.

TABLE 7: VETERAN'S BENEFITS DELIVERY NETWORK RECOVERY PRIORITIES

Priority	System Resource/Component	Recovery Time Objective
Website	BDN Web Site	<i>24 hours to rebuild or replace</i>
Application	Benefits Delivery Network - Education Systems Web Apps	<i>48 hours to rebuild or replace</i>
Application	Benefits Delivery Network - Payment History Web App	<i>72 hours to rebuild or replace</i>
Website	Benefits Delivery Network - Web Reports Site	<i>96 hours to rebuild or replace</i>

BIA Analysis:

Based on this BIA the BDN system is a moderate system because out of the four processes, two of them were moderate. The recovery time for the system resource/component is requiring

more than a 1-2 day recovery turnaround. Additionally, modest investments in recovery strategies should take place to ensure that this system resumes in a reasonable amount of time, that system components can be recovered, and that all information is adequately protected during a disruption.

VBA COMPENSATION AND BENEFITS SYSTEMS GRAPHIC

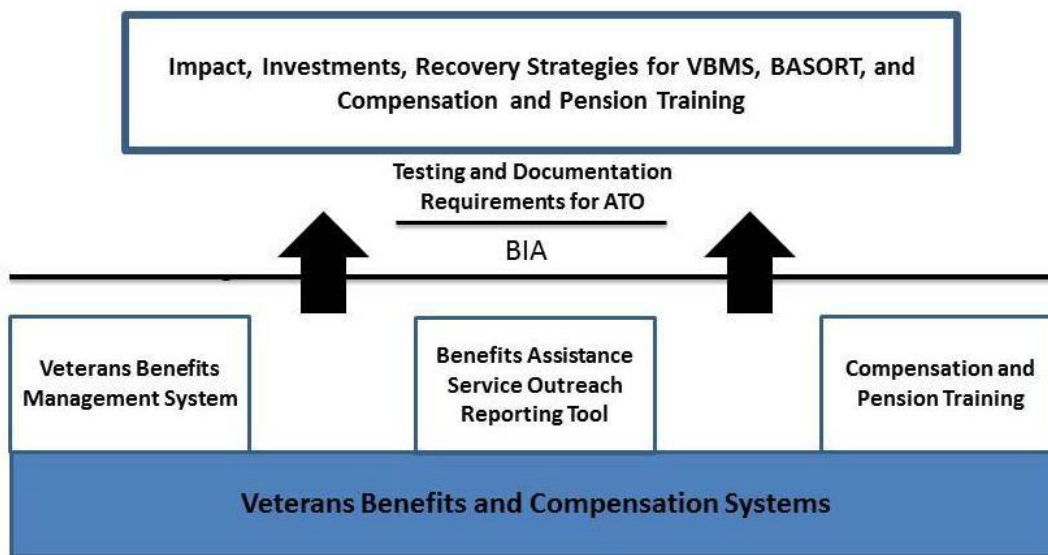


FIGURE 6: VETERAN'S BENEFITS AND COMPENSATION SYSTEMS BIA OUTPUTS

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.