2014-12

Business continuity management plan

Refugia, Manuel R., Jr.

Monterey, California: Naval Postgraduate School

`

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

BUSINESS CONTINUITY MANAGEMENT PLAN

December 2014

By: **Manuel R. Refugia Jr., and**
Gary O. Pittman

Advisors: **Douglass Brinkley,**
Man-Tak Shing

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2014	3. REPORT TYPE AND DATES COVERED MBA Professional Report

4. TITLE AND SUBTITLE BUSINESS CONTINUITY MANAGEMENT PLAN	5. FUNDING NUMBERS
6. AUTHOR(S) Manuel R. Refugia Jr. and Gary O. Pittman	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Naval Supply Systems Command 5450 Carlisle Pike P.O. Box 2050 Mechanicsburg, PA 17055-0791	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

Navy Supply Systems Command (NAVSUP) lacks a business process framework for the development of Business Continuity Management (BCM) plans. In the event business processes are deprived of automation for a prolonged period of time, the NAVSUP enterprise requires alternative methods to maintain the delivery of these products and services produced by these processes with minimum customer disruptions and financial losses. The purpose of this study was to review existing methodology to assess mission criticality of NAVSUP products and services and associated business processes. The analysis will lead to the development of a BCM plan and the associated information flow applied against a single Navy supply chain segment, Re-Engineered Maritime Allowance Development (ReMAD). This analysis will include recovery time and recovery point objectives. ReMAD and ERP interfaces as well as the ReMAD contingency plan will provide a context to lean on for the development of a business process framework for the plan. Currently, the ReMAD contingency plan's system recovery timelines and recovery point objectives are not sufficient to continue with the processing of Maritime allowances.

14. SUBJECT TERMS **TERMS** enterprise resource planning, re-engineered maritime allowance development, business continuity management			15. NUMBER OF PAGES 73
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

BUSINESS CONTINUITY MANAGEMENT PLAN

Manuel R. Refugia Jr., Lieutenant Commander, United States Navy
Gary O. Pittman, Lieutenant, United States Navy

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2014

Authors: Manuel R. Refugia Jr.

Gary O. Pittman

Approved by: Douglass Brinkley

Man-Tak Shing

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

BUSINESS CONTINUITY MANAGEMENT PLAN

ABSTRACT

Navy Supply Systems Command (NAVSUP) lacks a business process framework for the development of Business Continuity Management (BCM) plans. In the event business processes are deprived of automation for a prolonged period of time, the NAVSUP enterprise requires alternative methods to maintain the delivery of these products and services with minimum customer disruptions and financial losses. The purpose of this study was to review existing methodology to assess mission criticality of NAVSUP products and services and associated business processes. We focused on a single Navy supply chain segment, Re-Engineered Maritime Allowance Development (ReMAD). The ReMAD and ERP interfaces as well as the ReMAD contingency plan will provide a context to lean on for the development of a business process framework for the plan. Currently, the ReMAD contingency plan's system recovery timelines and recovery point objectives are not sufficient to continue with the processing of Maritime allowances. The analysis will lead to the development of a BCM plan for ReMAD that will meet the recovery time and recovery point objectives.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADM	allowance data manager
AHF	application hosting facility
APL	allowance parts list
BC	business continuity
BCA	business case analysis
BCI	Business Continuity Institute
BCM	business continuity management
BCP	business continuity plan
BIA	business impact analysis
CART	comparative analysis & research tool
CCQ	current calculated quantity
CDMD-OA	configuration data managers database-open architecture
CFO	chief financial officer
CI	control interface
CIO	chief information officer
COG	continuity of government
COOP	continuity of operations
DHS	Department of Homeland Security
DOD	Department of Defense
DODI	Department of Defense Instruction
DON	Department of the Navy
DR	disaster recovery
DRP	disaster recovery plan
ECG	enduring constitutional government
EDI	electronic data exchange

EHS	environmental, health and safety
ERP	Enterprise Resource Planning
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLC	Fleet Logistics Center
GAO	U.S. Government Accounting Office
GASB	Governmental Accounting Standards Board
GOTS	government off-the-shelf systems
GU	Griffith University
IA	information assurance
ISEA	in-service engineering activities
ISO	International Standardization Organization
IT	information technology
LSInc	Logistics Support, Incorporated
MAO	maximum acceptable outage
MEF	mission essential functions
MTD	maximum tolerable downtime
NIIN	national item identification number
NIST	National Institute of Standards and Technology
NSLC	Naval Sea Logistics Center
NAVSUP	Naval Supply Systems Command
POA&M	plan of action and milestone

ReMAD	Re-Engineered Maritime Allowance Development
RIC	repairable identification code
RPO	recovery point objective
RS	readiness suite
RTO	recovery time objective
SAFT	standard allowance file tool
SLA	service level agreement
SNAP	standard network access protocol
SNRA	Strategic National Risk Assessment
SNSL	Standard Navy Stock List
T-ART	targeted allowance reconciliation tool
TYCOM	type commander
UIC	unit identification code
UICP	Uniform Inventory Control Point
UPS	uninterrupted power supply
WSS	Weapons System Support

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We express our sincere gratitude to Dr. Douglas Brinkley and Dr. Man-Tak Shing for their unselfish dedication, guidance and wisdom in helping us achieve this milestone.

To CAPT Ré Bynum and CDR Brett Sullivan, thank you for your time and efforts in supporting our research project. Without your support we would not have been able to complete, let alone undertake, this project.

We also express our deepest appreciation to Mrs. Noel Yucuis and the Naval Postgraduate School Dudley Knox Library staff for their roles in providing us services in completing our research.

Finally, to our families, we express our deepest appreciation for your unconditional love and support throughout our project, especially Angela Pittman, and Dadey Refugia and Mamey Refugia. We thank you all for your patience and understanding through our journey while at Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

All organizations from public or private sectors face the possibility of disruptive events that have impacts ranging from mere inconvenience and short-lived disruption of normal business operations to the very destruction of the organization (Shaw, 2004). Navy Supply Systems Command (NAVSUP) does not have a framework that can help develop a business continuity management (BCM) plan. If business processes do not have automation for an extended period of time, the NAVSUP enterprise will need alternative procedures to maintain the delivery of the products and services produced by these processes with minimum customer interruptions and fiscal losses. The purpose of this study is to analyze the existing NAVSUP products and services and associated business processes to identify the information necessary to continue the delivery of the critical process elements, and develop BCM and the associated information flow. This analysis will help with the development of a BCM framework applied against a Navy supply chain segment that will include recovery time and recovery point objectives.

Navy Enterprise Resource Planning (ERP) is an integrated business management system that updates and standardizes Navy business operations, provides financial transparency and total asset visibility across the enterprise, and increases effectiveness and efficiency. ERP is the generic name of a software-based management system used by forward-leaning corporations around the world to power their crucial "back office" business functions. The Navy ERP Program uses a product from SAP Corporation, which allows the Navy to unify, standardize, and streamline all its business activities into one completely integrated system. The first release of the system, implemented in October 2007, focused on core financial and acquisition processes. The second release of the system in February 2010 added wholesale and retail supply business processes. Successful Navy command implementation of this business management system requires carefully planned and organized phased activities with specific timelines, sequences, and deliverables. Implementation guidance for Navy ERP provides details of the process and key information on structuring a command's teams and efforts for success. It also

identifies critical success factors and provides timelines and checklists to help focus a command's resources.

B. PURPOSE

The purpose of this study is to develop a framework that NAVSUP can use to create a BCM plan that can help maintain the continuity of business processes with minimal customer disruptions and financial loss. In some way, the business process meets a requirement by delivering a product or service that sustains or improves readiness.

The goal of a BCM is to provide the organization with the ability to effectively respond to threats such as natural disasters or data breaches and protect the business interests of the organization. BCM includes disaster recovery. The allowancing process, Reengineered Maritime Allowance Development (ReMAD) and ERP interfaces will give us a context to lean on as we develop the business process framework for the plan. These were chosen to provide structure and scope for the project. A good framework can be expanded in response to business process complexity and how and where the process is performed. In the end, it is about the readiness of operational forces, so a good BCM should answer a few questions.

C. RESEARCH QUESTIONS

Now we will discuss primary and secondary questions that should be considered when developing a framework for a BCM plan. This list is not exclusive, because it should be tailored to the organization's requirements.

1. Primary

- What are the most likely threats to this business process? Can we mitigate the threats and vulnerabilities prior to an event?
- What is the impact to readiness?
- What are the key decision and plan of action and milestone (POA&M) points?

- At what point after an event does the process owner have to initiate the BCM?
- What are the key lead times for critical POA&M points?

2. Secondary

- How does the exploitation of the business process vulnerability affect the ways and means we deliver the requirement?
- Does the event drive a change in our business process temporarily (think manual processing) or permanently (think additional information assurance (IA), physical security or background investigation requirements)?
- How will accountability be maintained during BCM plan execution?

D. ROLES AND RESPONSIBILITIES

Senior management will have ultimate responsibility for creating and implementing the BCM plan. A BCM team leader should be designated in writing to carry out the approved plan with the assistance of the process owners. They must ensure that the BCM plan is written and distributed so several groups of people can help with the execution in a timely fashion (Griffith University [GU], 2013). It should be precise about what situations can prompt initiation of the plan. It should state the immediate steps to be taken whenever a disruption occurs. The plan should include an inventory of vital assets and resources needed to support critical processes. It should allow flexibility for the business to respond to unexpected threat situations and varying internal environments. Ultimately, management should ensure that the BCM plan's main focus should be on how to get the business back online in regards to a specific capability, and work area or role that is interrupted, rather than on the exact nature of the disruption. Senior management and the BCM team leader are responsible for ensuring that the BCM plan is readily available to all process owners in electronic and hard copy formats on and off-site (GU, 2013). Figure 1 displays an example of a BCM team organization chart that Federal Emergency Management Agency (FEMA) uses for a BCM framework (FEMA, 2014a).

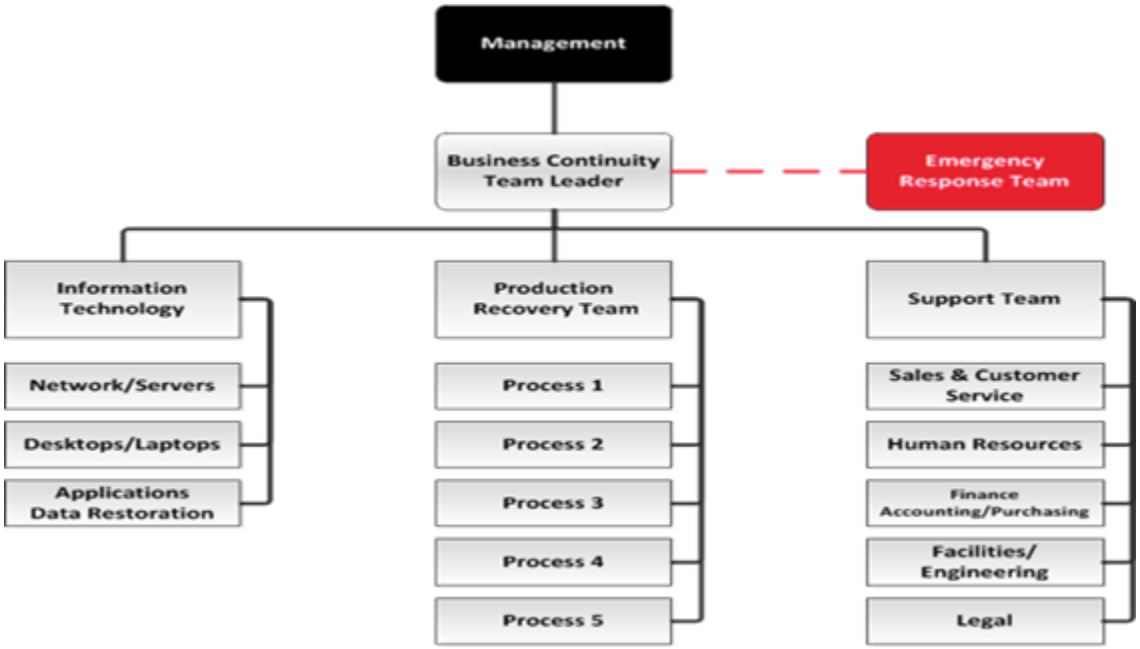

Figure 1. Business Continuity Team Organization Chart (from FEMA, 2014a)

The organization chart covers essential team members for developing a successful plan. A BCM plan should clearly define and appropriately assign the roles and responsibilities of all stakeholders. The management and team members should collaborate to identify their critical strengths in the organization and recognize which weaknesses are important. Lines of authority, sequence of management, and delegation of authority must be identified to ensure the successful development and implementation of the BCM plan. They must also address communication with outside organizations including contractors and vendors (FEMA, 2014a).

II. RE-ENGINEERED MARITIME ALLOWANCE DEMAND

A. OVERVIEW

The purpose of this chapter is to give an example of a Navy supply chain segment to highlight the needs for a BCM plan. This chapter will give a brief synopsis of what ReMAD is used for and the some basic functional interfaces used by the NAVSUP enterprise. ReMAD and ERP interfaces along with the ReMAD contingency plan will provide context that can be used to develop the business process framework for the BCM plan.

B. DEFINITION OF REMAD

The ReMAD system was developed for the Department of the Navy (DON), Naval Supply Systems Command (NAVSUP), and NAVSUP Business Systems Center (BSC). This system is a web-based, maritime parts-allowance support tool used by type commanders (TYCOM), as well as the NAVSUP enterprise. It is a government off-the-shelf (GOTS) system that utilizes commercial application software modified to fulfill unique core—NAVSUP WSS mission requirements (NAVSUP, 2008). The users of the system include the operating sites: NAVSUP Weapon Systems Support (WSS) Allowancing, NAVSUP Allowancing Support, Naval Sea Logistics Center (NSLC) budget support, type commanders (TYCOM) platform managers, NAVSUP program managers, In-service engineering activities (ISEAs), supply officers, and other fleet personnel. Of particular importance, ReMAD augments Navy ERP designs by providing the sole means for fleet (i.e., shipboard/activity/ installation) allowances determination once legacy uniform inventory control point (UICP) processing is terminated (NAVSUP, 2012).

C. BACKGROUND

ReMAD is the allowancing process used by NAVSUP WSS to achieve its core mission, which is to identify spare parts needed to repair Navy ships and weapon

systems. Existing maintenance products provide allowances based on partial information, and the current system needs a manual review of allowances (NAVSUP, 2008).

ReMAD is a redesign and re-host maritime allowance calculation process that is web-based unlike its predecessor. The system has functionality improvements that can be used to increase platform readiness. It has a direct link to key data sources as well as automation that can help with other functions such as funds control and quality assurance. There is web access for the TYCOM and NAVSUP WSS. Another function that is available is the ability to conduct ad hoc queries and scenario based analyses. ReMAD can also interface with ERP for data and allowance distribution (NAVSUP 2008).

Logistics Support, Incorporated (LSInc), a premier global provider of responsive management consulting, and logistics solutions, is the prime contractor that delivers support to NAVSUP WSS Mechanicsburg to create and refine requirements, documentation, testing, and implementation of the ReMAD system and its interface with ERP (LSInc, 2014). LSInc provides skill and knowledge of the allowance process and fleet interface including the ERP single supply solution, and other related program-level requirements. They also provide training on various aspects of allowancing and ReMAD to both government and contractor personnel (LSInc, 2014).

Figure 2 displays the various inputs and outputs that ReMAD processes (NAVSUP, 2008). Some of the outputs interact with the ERP system as shown.

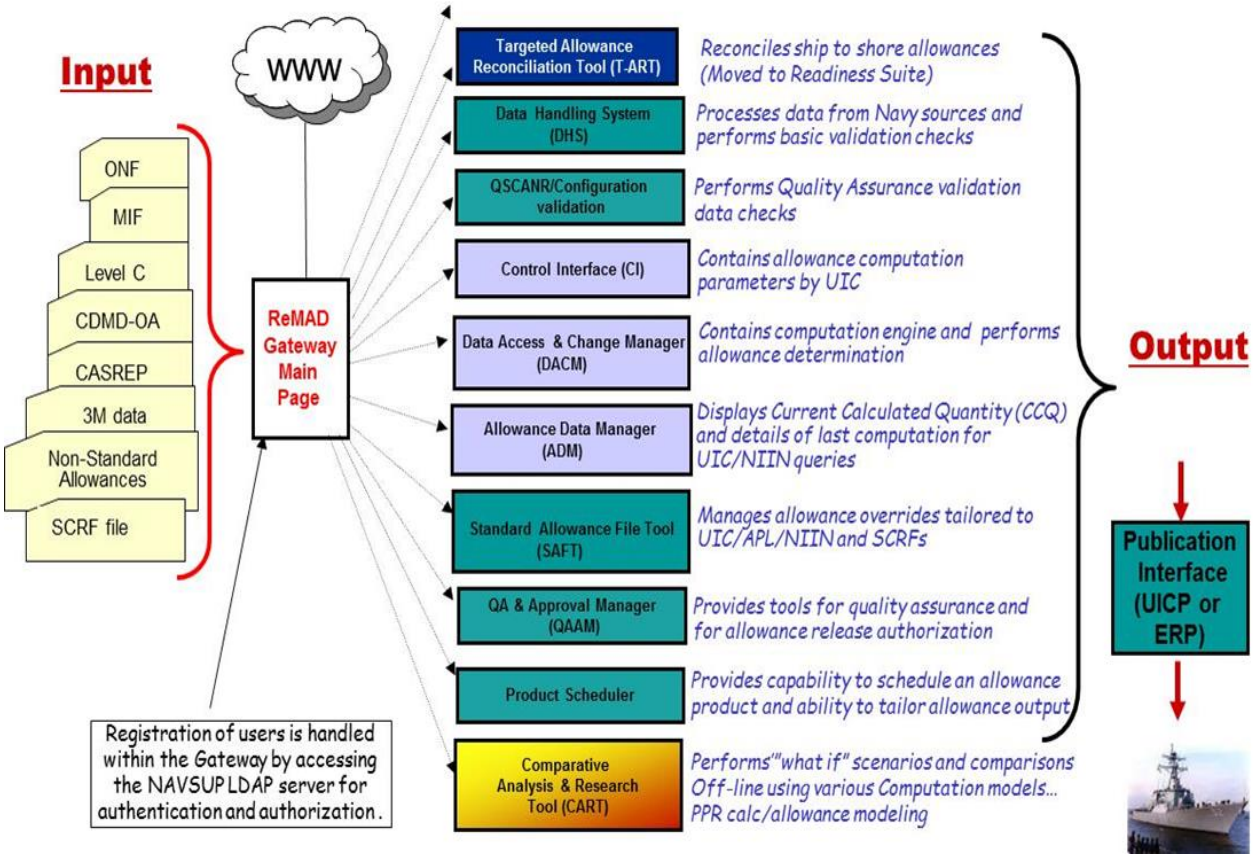

Figure 2. ReMAD inputs and outputs (from NAVSUP, 2008)

Below are some of the inputs and outputs (NAVSUP, 2008):

Input to ReMAD from ERP

- WSF-C allowance parts list (APL)-National Item Identification Number (NIIN data)
- Old NIIN file (NIIN supersessions and cancellations)
- Repairable identification code (RIC) supersessions and cancellations
- Parent to accessory RIC data

Output from ReMAD to ERP

- Records for SNAP unit identification codes (UIC)
- Specific format for non-automated UICs
- Authorized allowances
- Allowance deletions
- Allowance projections

A discussion of the functional interfaces that exist between ERP and other systems is shown. The following describes how they all interact (Krause, 2010):

- ERP will be the repository of RIC to NIIN data
- RIC & NIIN information in WSF will reside in ERP
- ERP will pass data to ReMAD, Readiness Suite and CDMD-OA
- ReMAD will (Krause, 2010):
- Perform maritime data validation, allowance computation, product scheduler, quality assurance and distribution vehicle
- Store historical allowance information
- Perform special allowance processes

  Receive data from and pass final allowance, sales order and sales quotes to ERP

Readiness Suite (RS) will:

- Perform calculations and support the retail allowance products
- Perform effectiveness studies
- Receive data from and pass sales quotes to ERP (for some products)

CDMD-OA will (Krause, 2010):

- Receive APL/NIIN and allowance data from ERP
- Access the CAPs web page for product order info
- Create allowance product text files
- Distribute allowance product text files
- Create CD-ROMs to DAPS
- Post Data transfer to Text files

InforM-21 will:

- Receive allowance related information from ReMAD
- Perform Ad-hoc queries and reports

Figure 3 displays a block diagram of ReMAD and the various systems that interact with each other (Hynosky, 2010).

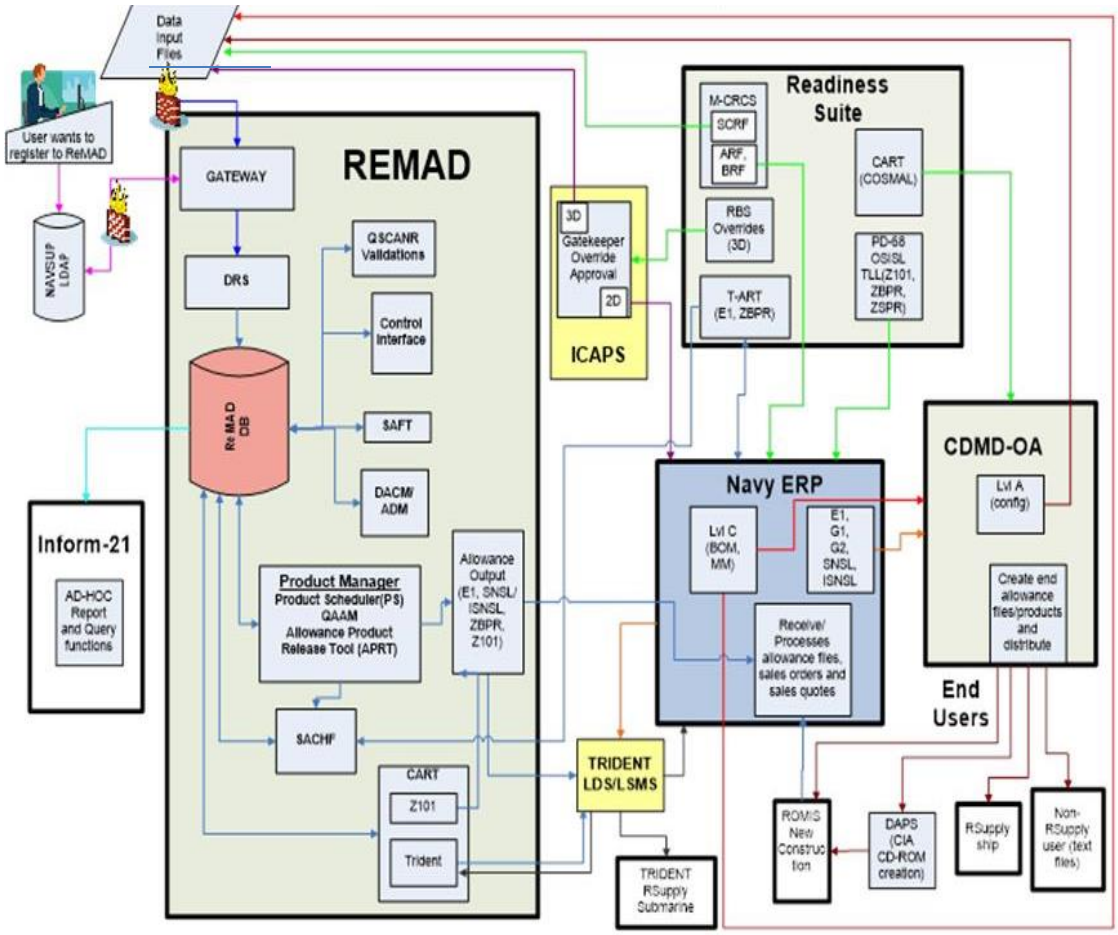

Figure 3. Maritime Allowance System (from Hynosky, 2010).

D. CONTINGENCY PLAN

The purpose of the ReMAD Contingency Plan is to establish procedures to recover the system following a disruption (NAVSUP, 2012). The plan should include the following phases: the notification and activation phase that can detect, assess damage and the actual activation of the contingency plan. The recovery phase should be used to restore temporary IT operations and alleviate the effects that were caused by the damage to the original system. During the reconstitution phase, all capabilities should be restored to normal operations. All procedures and resources needed to continue normal business operations should be identified. Personnel should be designated and guidance provided to them on how to recover ReMAD during extended periods of interruption to normal operations. Ongoing coordination with all staff involved in the contingency planning is

an essential requirement for the plan to be a success as well as coordination with external points of contact who are involved in the contingency planning strategies (NAVSUP, 2012).

The ReMAD contingency plan applies to all functions and resources required in restoring continuity of operations at the Application Hosting Facility (AHF), Tulsa, Oklahoma. This contingency plan was established based on multiple assumptions. An example scenario used was the inaccessibility of the AHF. NAVSUP BSC/NAVSUP WSS/NAVSUP would be unable to perform an analysis using ReMAD (NAVSUP, 2012). The following are some key assumptions that were made when the plan was developed (NAVSUP, 2012). ReMAD operations have been interrupted at the AHF computer center and will not be available within 48 hours/ two weeks/ two months. Essential ReMAD personnel have been identified and trained in their emergency response and recovery roles and they are readily available to activate the ReMAD Contingency Plan. Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) have full operational capability whenever the disaster occurs (NAVSUP, 2012). Based on the 2012 contingency plan:

> Computer center equipment, including components supporting ReMAD, is linked to an uninterruptible power supply (UPS) that can provide 45 minutes to 1 hour of power during power failure. The AHF cannot provide hardware and software support for ReMAD for at least 48 hours. An emergency evacuation of personnel at the AHF if inaccessible for at least 48 hours should be activated. The blockhouse is the alternate site with trained personnel to assist in operation of ReMAD. Current backups of the application software and data are undamaged and accessible at the offsite storage facility. Agreements for service are maintained with ReMAD hardware, software, and communications providers to provide support to restore ReMAD to normal operations (NAVSUP, 2012).

The plan establishes numerous teams to recover ReMAD operations. The specific actions performed by these teams are stated in the ReMAD contingency plan as well as detailed steps of the notification, activation, recovery and normal phase. The recovery timelines and recovery point objectives for the ReMAD system contingency plan cannot provide the support needed to continue with the processing of maritime allowances. The

following section cites two case studies that demonstrate how an organization mitigated issues during catastrophic events that led to disruptions to their business operations.

E. INDUSTRIAL CASE STUDIES

Valuable lessons can be learned from past experiences of others as well as industry best practices. Due to the fact that the following companies had adequate preparations for their organizations for untimely disturbances, they were not faced with prolonged interruptions to their business operations.

a. Morgan Stanley

In 1993, when terrorists initially attacked the World Trade Center, Morgan Stanley, a financial services company, learned a life-saving experience. It took the company four hours to evacuate its employees, some of whom had to walk down 60 or more flights of stairs to areas of safety. None of their employees were killed in the attack, but the company's management decided their disaster plan was insufficient. They conducted a thorough risk assessment of their current plan, performed an analysis of a potential disaster risk and developed a multi-faceted disaster plan. Perhaps just as importantly, they practiced the plan frequently to provide for employee safety in the event of another disaster (FEMA, 2014c).

On September 11, 2001, the planning and training brought excellent dividends. As soon as the first hijacked plane collided with One World Trade Center, Morgan Stanley security executives ordered the company's 3,800 employees to evacuate from World Trade Center buildings, Two and Five. It only took 45 minutes for all employees to get out to safety (FEMA, 2014c).

Due to effective crisis management and communication, Morgan Stanley was prepared to offer grief counseling to workers and increased its security presence. It also used effective communications strategies to provide timely, appropriate information to management and employees, investors and clients, and regulators and the media (FEMA, 2014c).

Although Morgan Stanley had 13 casualties, many more could have died if the company had not had a solid disaster plan that was practiced over and over again during numerous training sessions. In making a commitment to prepare its most valuable asset, its people, Morgan Stanley ensured the firm's future (FEMA, 2014c).

b. John Deere

"Safety and security of employees has always been a major priority for our company," stated Allen Steinbeck, Director of John Deere Worldwide Security/Aviation. One of the oldest manufacturing companies in the United States, John Deere, is making emergency preparedness a company priority. Steinback is a member of the team that created the National Fire Protection Association's (NFPA) 1600 standard on disaster/emergency management and business continuity. He utilized his experience and knowledge to help develop and implement best practices within John Deere (FEMA, 2014c).

Steinback stated, "planning for critical incidents and training employees on proper emergency procedures should become a standard throughout any business model," and "The NFPA 1600 standard was instrumental in helping our security team identify the specific areas where our emergency plans needed to be enhanced (FEMA, 2014c).

John Deere Worldwide Security has hired regional security managers working with an emergency preparedness manager (EPM) to ensure that all its elements have comprehensive and updated emergency action procedures that follow the corporate crisis management plan and the NFPA 1600 standards. The EPM is accountable for all emergency training, initiating a pandemic plan, recognizing and implementing best-practices, obtaining technology to handle critical incidents, and various other emergency preparedness duties (FEMA, 2014c).

Through extensive planning, preparation and training a company can possess the key elements for effective mitigation of an actual or potential crisis. All organizations should become familiar with current standards and remain diligent in implementing the applicable plan for their circumstances (FEMA, 2014c).

III. BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

The details of how to develop a BCM framework will be discussed in this chapter. According to Protiviti, the development of strategies, policies and procedures set the foundation for a good BCM plan. This provides security or alternative methods of operation for business processes. If these processes were interrupted, the enterprise could suffer severe damage or significant loss that could be difficult to recover from. A BCM plan should be composed of the following three elements: crisis management and communications, business recovery planning, and information technology (IT) disaster recovery (DR) (Protiviti, 2013).

A. RISK ASSESSMENT

Business Continuity Institute suggests that a management plan can be constructed from the BCM framework in Figure 4 (Business Continuity Institute [BCI], 2014a). Risk assessment can be defined as recognizing and prioritizing threats and disaster scenarios to which the enterprise may be vulnerable. Most risk management programs utilize a risk assessment tool to identify and prioritize threats, risks and failure scenarios. A BCM program incorporates these risk management strategies along with other methods to keep the business functioning whenever an event occurs and threatens essential business processes. Within BCM, a wide variety of risk management procedures are used; most classify and prioritize risk using a combination of likelihood (probability) and severity (impact). In addition to likelihood and severity, additional characteristics that may be factored into the prioritization effort are detectability and velocity to impact (BCI, 2014a).

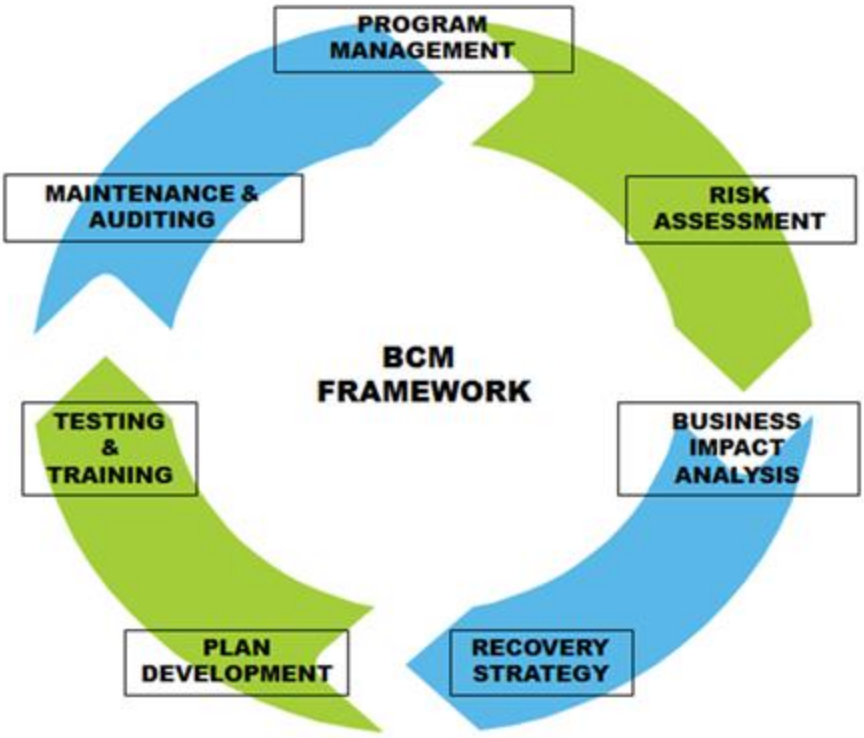

Figure 4. Business Continuity Framework Model

Now that a good framework model has been presented, we will discuss the different types of risks that an enterprise could possibly face. The risk environment affecting critical infrastructure is complex and uncertain; threats, vulnerabilities, and consequences have all evolved over the last 10 years (Department of Homeland Security [DHS], 2011). DHS stated that the strategic national risk assessment (SNRA) describes numerous threats and susceptibilities to business processes in the extensive types of man-made, natural, and technical threats. Critical resources, business systems, and networks face many of the threats characterized by the SNRA, including terrorists and other people trying to cause damage and interrupt vital services through physical and cyber-attacks, natural disasters, pandemic viruses or other health emergencies. The potential for interrelated events with unlimited consequences increases uncertainty as well as the identified risks evaluated as part of the SNRA (DHS, 2011). Figure 5 describes the evolving threats (DHS, 2013).

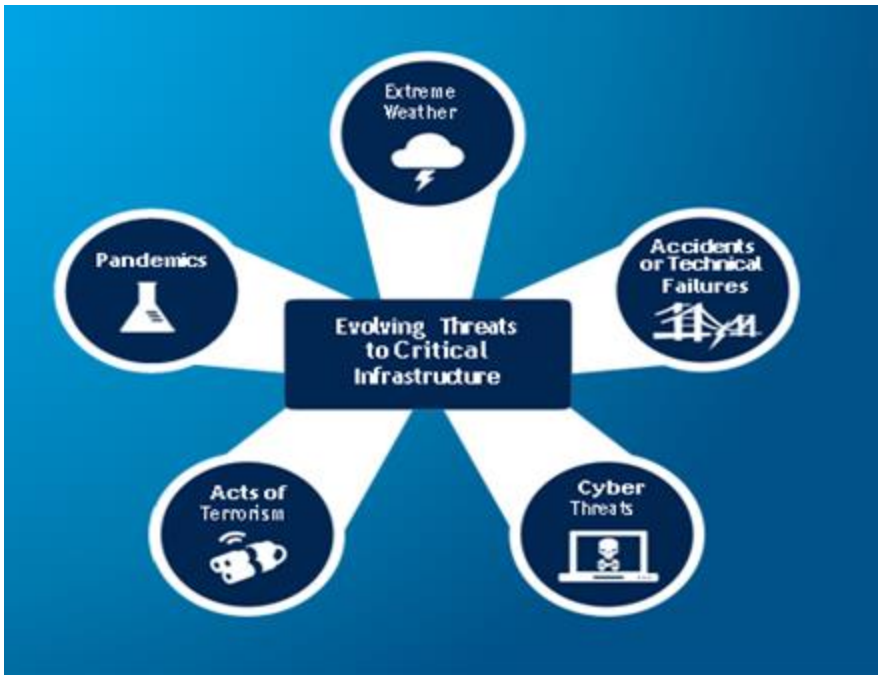

Figure 5. Evolving Threats to Critical Infrastructure (from DHS, 2013)

Rising interdependencies across critical infrastructure systems, mainly dependence on data and communications technologies, have amplified the possible weaknesses to physical and cyber dangers and potential fears resulting from the compromise of essential systems. Critical infrastructure crosses domestic boundaries and international supply chains in a unified world. Due to our interdependence on technology, we can be greatly impacted by a diverse set of dangers (DHS, 2013).

In addition, the effects of dangerous elements could threaten critical infrastructure that provides necessary services to the domestic population. Current and future variations to the environment have the potential to compound these dangers and could have a key effect on infrastructure processes. Lastly, susceptibilities also may occur as a result of a retiring work force or deficiency of experienced labor. Skilled operators are required for infrastructure upkeep and, hence, security and flexibility. Numerous issues impact the risk environment and, along with the policy and functioning environments, create the setting against which choices are made for critical infrastructure safety and resilience (DHS, 2011). Figure 6 provides a good example of how to assess risk (FEMA, 2014a).

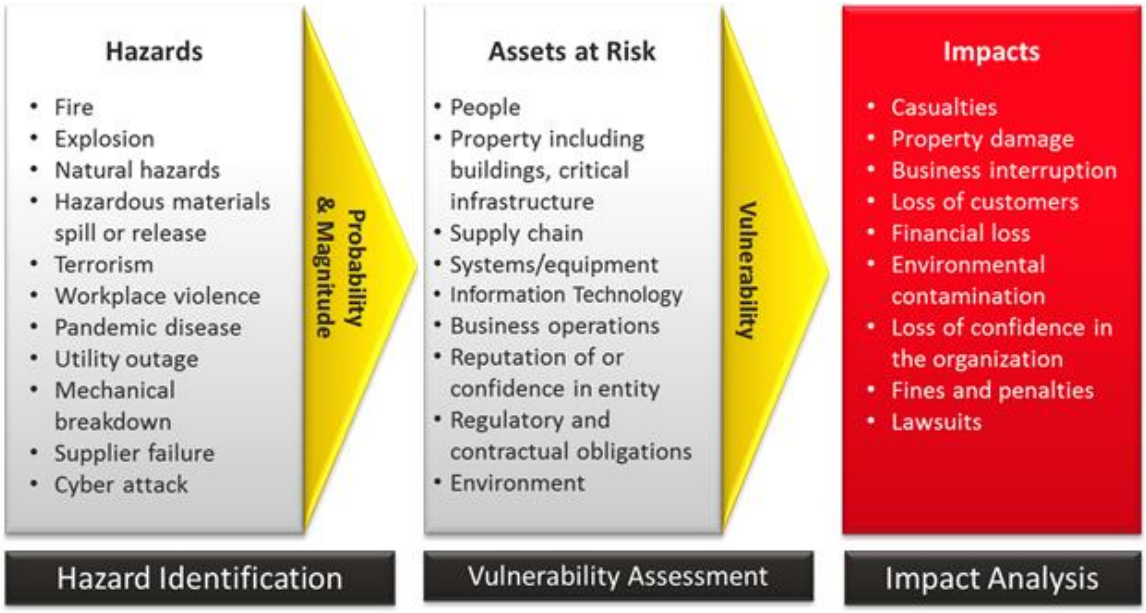

Figure 6. Risk Assessment Chart (from FEMA, 2014a)

Next we discuss how to assess and analyze the risks. Critical infrastructure can be assessed in three categories: threat, vulnerability, and consequence. A threat is a natural or manufactured event or action that can possibly pose a threat to life, information, operations, the environment and property (DHS, 2013). Vulnerability is a physical feature or operational characteristic that renders an entity exposed to exploitation or susceptible to a given threat. A consequence is the effect of an event, incident, or occurrence. DHS mentions in a 2013 study that risk assessments are conducted by many critical infrastructure partners to inform their own decision making, using a wide variety of methodologies. These assessments permit critical infrastructure managers to comprehend the most likely and severe events that could disturb their operations and use this information to support preparation and resource allocation in a coordinated fashion. To assess risk successfully, critical infrastructure partners (owners and operators) need timely, dependable, and actionable data regarding threats, vulnerabilities, and consequences. Partners should comprehend intelligence and information requirements and conduct joint analysis where appropriate. In order to understand the risk to cyber and physical systems and assets, an assessment must be performed by the various members of the partnership. Neither public nor private sector entities can fully comprehend risk

without this integration of comprehensive knowledge and analysis (DHS, 2013). The Federal Emergency Management Agency (FEMA) provides tools such as the Ready Business program to help managers and their workforce focus on business preparedness. Table 1 is an example of one of those tools that can be adapted by an organization for risk assessment (FEMA, 2014a).

(1) Asset or Operation at Risk	(2) Hazard	(3) Senario (Location, Timing, Magitude)	(4) Oportunities for Prevention or Mitigation	(5) Probability (L, M, H)	Impacts with Existing Mitigation (L, M, H)					(11) Overall Hazard Rating
					(6) People	(7) Property	(8) Operations	(9) Environment	(10) Entity	

Table 1. Risk Assessment Table (from FEMA, 2014a)

B. BUSINESS IMPACT ANALYSIS

Business impact analysis (BIA) is the process an organization uses to identify which functions are critical to the business and to ascertain the maximum acceptable outage (MAO) period for each identified function (BCI, 2014a). A comprehensive BIA should assess all key inputs and outputs for critical processes (Protiviti, 2013). The BIA is the second step in business continuity management cycle to identify and prioritize critical functions following a disruptive event, in order to achieve minimum service

delivery and identify resources required to aid in resumption of function after disruption. Outputs of this step include written reports describing probability of significant threats, the consequences of threat realization on the business process, and prioritization of the threats based on the likelihood of the consequences (NAVSUP, 2011a). BIA results determine how critical the system is to the supported mission and business processes, what impact the loss of the system could have on the organization, and the system recovery time objective (RTO). The BIA results can help determine the type and frequency of backup, the need for redundancy or mirroring of data, and the type of alternate site needed to meet system recovery objectives (Swanson, Bowen, Phillips, Gallup, and Lynes, 2013). The purpose of the BIA is to associate the system with the critical mission or business processes and services provided and identify the consequences of a disruption. The BIA process will vary based on industry dynamics, business complexity, use of technology, frequency of change, and management style. The four main elements are (Protiviti, 2013):

1. **Scoping**—This includes IT and/or business functions which may be internally focused, or may include critical business partners, vendors and customers. The scope of the BIA drives all succeeding analytic efforts.
2. **Data collection**—Data collection is most effective when prepared in group-facilitated sessions and individualized interviews. The use of surveys and a review of management reporting can be efficient method as well.
3. **Analyzing**—in some organizations, quantitative impacts drive the process, whereas in others, qualitative impacts are just as important. Types of impacts that should be considered include:
    a. Work stoppage and idle workforce
    b. Regulatory violations or noncompliance
    c. Financial loss or delay
    d. Loss of stakeholder confidence
    e. Reputation impairment
    f. Environmental, health and safety (EHS) impairment
    g. Cash flow interruption
    h. Financial control and reporting exposure
    i. Customer service and strained vendor relations

j. Employee morale/retention

k. Service level agreement (SLA) /contractual noncompliance

4. **Reporting**—Text versus graphs, reports versus presentations. Corporate culture and audience should determine the exact format to ensure BIA findings are understood and actionable.

The BIA results must be acknowledged by the executive management team before the rest of the BCM project can effectively take place. During impact analysis, each vulnerability needs to be rated based on the likelihood and consequence or impact in order to determine the vulnerability risk rating (NAVSUP BSC, 2011). The decision of which scale to use is insignificant. The important point is to use a risk rating that is a consistent and well defined scaling method within a capability. This enables the accurate and consistent prioritization of the vulnerabilities for future planning purposes. During prioritization, the extreme, high, or critical ratings represent vulnerabilities that must be addressed. The moderate or medium ratings may or may not be mitigated depending on the costs associated with the solution. Mitigation strategies are not normally established for low ratings unless the costs are minimal and the solution is easily implemented.

The five-point matrix (Figure 7) uses likelihoods of rare, unlikely, moderate, likely and almost certain and consequences of insignificant, minor, moderate major and catastrophic (NAVSUP BSC, 2011).

LIKELIHOOD	CONSEQUENCES				
	INSIGNIFICANT Minor problem easily handled by normal day to day processes	MINOR Some disruption possible)	MODERATE (Significant time/ resources required)	MAJOR (Operations severely damaged)	CATASTROPHIC (Operations survival is at risk)
DAMAGE COST ESTIMATE	**<$500k**	**$500k**	**$1 million**	**$10 million**	**$25 million**
Almost certain >90% chance	**HIGH**	**HIGH**	**EXTREME**	**EXTREME**	**EXTREME**
Likely Between 50% and 90% chance	**MODERATE**	**HIGH**	**HIGH**	**EXTREME**	**EXTREME**
Moderate Between 10% and 50% chance	**LOW**	**MODERATE**	**HIGH**	**EXTREME**	**EXTREME**
Unlikely Between 3% and 10% chance	**LOW**	**LOW**	**MODERATE**	**HIGH**	**EXTREME**
Rare <3% chance	**LOW**	**LOW**	**MODERATE**	**HIGH**	**HIGH**

Figure 7. Five-point Matrix (from NAVSUP BSC, 2011)

The three-point matrix (Figure 8) uses low, medium and high for both likelihood and consequence (NAVSUP BSC, 2011).

HIGH	**MEDIUM**	**HIGH**	**CRITICAL**
MEDIUM	**LOW**	**MEDIUM**	**HIGH**
LOW	**LOW**	**LOW**	**MEDIUM**
	LOW	MEDIUM	HIGH

Figure 8. Three-point Matrix (from NAVSUP BSC, 2011)

C. RECOVERY STRATEGY

Recovery strategy is the third step in the BCM cycle which will be based on the results of the BIA. In order to develop a solid recovery strategy, the capability leadership team must have a thorough understanding of the capability processes. A recovery strategy focuses on maintaining the mission regardless of what is or is not available such as IT

services, facilities, infrastructure, personnel, etc. (NAVSUP, 2011a). The output of this step is a written report outlining the vulnerabilities and threats requiring action along with a description of the mitigation plan and/or contingency plan along with a breakdown of the cost requirements. For the purpose of this report, contingency plan will not be thoroughly discussed. Determination and selection of strategy is based on outputs from the BIA, and built upon the maximum acceptable outage (MAO) identified for each critical process. Senior management will determine appropriate business continuity strategy in order to (GU, 2013):

1. Protect core functions and critical business processes;

2. Stabilize, sustain, recover and restore functions, services, critical processes and their dependencies and supporting resources.

Response strategy will be informed by approved time frames for recovery of critical processes. There are three ways to identify downtime (NAVSUP, 2011b):

1. Maximum tolerable downtime (MTD). The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with inaccurate direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

2. Recovery time objective (RTO). RTO is the target time for resuming the delivery of a product of service to an acceptable level following its disruption (GU, 2013). It 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. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a plan of action and milestone (POA&M) should be initiated to document the situation and plan for its mitigation.

3. Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD.

Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

When selecting response strategies the following should be considered:

- The type of hazard(s) the group is exposed to;
- Alternate procedures for carrying out the process to completion or to a minimum;
- Acceptable level until recovery can be effected;
- Manual processing abilities and related costs;
- Use of insurance (replace rather than salvage—if applicable);
- Third party arrangements, business partnering/dependencies, sector mutual aid;
- Business cycles and peak periods;
- Internal resource capabilities, critical supply chains and vendor management;
- Deciding whether or not an alternative site is required;
- Accessibility of data;
- The option to do nothing—deciding how much the business can afford to lose

If a facility is damaged, production machinery breaks down, a supplier fails to deliver or information technology is disrupted, business is impacted and the financial losses can begin to grow. Recovery strategies are alternate means to restore business operations to a minimum acceptable level following a business disruption and are prioritized by the RTO developed during the business impact analysis.

Recovery strategies require resources including people, facilities, equipment, materials and information technology. An analysis of the resources required to execute recovery strategies should be conducted to identify gaps. For example, if a machine fails

but other machines are readily available to make up lost production, then there is no resource gap. However, if all machines are lost due to a flood, and insufficient undamaged inventory is available to meet customer demand until production is restored, production might be made up by machines at another facility—whether owned or contracted.

Strategies may involve contracting with an outside firm, entering into partnership or reciprocal agreements. The Defense Information Systems Agency (DISA), provides remote recovery capability, or continuity of operations (COOP) in accordance with standards and regulatory requirements outlined in DOD Instruction (DODI) 8500.2 including continuity—related information assurance (IA) controls. For disaster and recovery planning, DISA ensures plans and procedures exist to allow resumption within required time frames (DISA, 2014).

Also consider manual processing options, or establishing a remote, redundant site for mission—critical operations, which will be composed of staff with in-depth knowledge of business functions and processes that are in the best position to determine what will work.

Vin D'Amico, an agility expert on business continuity planning states that possible alternatives should be explored and presented to management for approval and to decide how much to spend (2004). Depending upon the size of the company and resources available, there may be many recovery strategies that can be explored.

Utilization of other owned or controlled facilities performing similar work is one option. Operations may be relocated to an alternate site—assuming both are not impacted by the same incident. This strategy also assumes that the surviving site has the resources and capacity to assume the work of the impacted site. Prioritization of production or service levels, providing additional staff and resources and other action would be needed if capacity at the second site is inadequate.

Telecommuting is a strategy employed when staff can work from home through remote connectivity. It can be used in combination with other strategies to reduce alternate site requirements. This strategy requires ensuring telecommuters have a suitable

home work environment and are equipped with or have access to a computer with required applications and data, peripherals, and a secure broadband connection.

In an emergency, space at another facility can be put to use. Cafeterias, conference rooms and training rooms can be converted to office space or to other uses when needed. Equipping converted space with furnishings, equipment, power, connectivity and other resources would be required to meet the needs of workers.

Partnership or reciprocal agreements can be arranged with other businesses or organizations that can support each other in the event of a disaster. Assuming space is available, issues such as the capacity and connectivity of telecommunications and information technology, protection of privacy and intellectual property, the impacts to each other's operation and allocating expenses must be addressed. Agreements should be negotiated in writing and documented in the business continuity plan. Periodic review of the agreement is needed to determine if there is a change in the ability of each party to support the other.

There are many vendors that support business continuity and information technology recovery strategies. External suppliers can provide a full business environment including office space and live data centers ready to be occupied. Other options include provision of technology equipped office trailers, replacement machinery and other equipment. The availability and cost of these options can be affected when a regional disaster results in competition for these resources.

There are multiple strategies for recovery of manufacturing operations. Many of these strategies include use of existing owned or leased facilities. Manufacturing strategies include:

- Shifting production from one facility to another
- Increasing manufacturing output at operational facilities
- Retooling production from one item to another
- Prioritization of production—by profit margin or customer relationship
- Maintaining higher raw materials or finished goods inventory
- Reallocating existing inventory, repurchase or buyback of inventory

- Limiting orders (e.g., maximum order size or unit quantity)
- Contracting with third parties
- Purchasing business interruption insurance

The following factors should be considered in manufacturing recovery strategies:

- Will a facility be available when needed?
- How much time will it take to shift production from one product to another?
- How much will it cost to shift production from one product to another?
- How much revenue would be lost when displacing other production?
- How much extra time will it take to receive raw materials or ship finished goods to customers? Will the extra time impact customer relationships?
- Are there any regulations that would restrict shifting production?
- What quality issues could arise if production is shifted or outsourced?
- Are there any long-term consequences associated with a strategy?

D. PLAN DEVELOPMENT

Software is not required to develop a good BCM plan but it can be a helpful tool. Most organizations decide to create a BCM plan utilizing normal, word-based templates typically used by smaller and medium-sized, single-site organizations. Though, a rising number of businesses, mainly larger, geographically isolated organizations, are choosing to implement software solutions to develop plans, manage content and distribute updated plan documentation. Furthermore, some organizations are using pre-existing tools such as SharePoint to establish, share and maintain BCM plans (Protiviti, 2013). Figure 9 displays a business continuity planning process diagram that can be used for plan development (FEMA, 2014a).

Figure 9. Business Continuity Planning Process Diagram (from FEMA, 2014a)

Even though software solutions can add value, managers should address three important concerns to make the investment payoff (Protiviti, 2010):

1. Recognize that software and template customization is needed before implementation and use. Purchasing software does not mean the organization is purchasing a plan.

2. Access controls should be implemented to protect sensitive information and adhere to privacy concerns.

3. "Fantasy plans" can create a false sense of security. Organizations that acquire business continuity software tools must beware of the "solution in a box" syndrome. A tool set can be a great aid, but the development of effective business resumption or IT disaster recovery plans requires people with the right skills and experience.

Resource management is a vital part of the BCM plan that is used to ensure the business has the resources needed to be properly prepared. Those resources include (Protiviti, 2013):

- People
- Facilities
- Communications and warning technologies
- Fire protection and life safety systems
- Pollution control systems
- Equipment
- Materials and supplies

- Funding
- Special expertise
- Information about the threats or hazards

If a primary facility cannot be used for normal business operations, an appropriate alternate facility can be used until the primary facility is back online. The alternate facility is considered a resource for the business continuity plan (Protiviti, 2010).

A needs assessment should be performed to decide what resources are needed. Resources may derive from within the business and may be comprised of trained employees, protection and safety systems, communications equipment and other services owned or leased by the business. External resources such as public emergency services, business partners, vendors and contractors are essential in preparing and developing the BCM plan (Protiviti, 2010).

The accessibility and capability of resources must be determined because some resources might be required immediately. The availability of resources often hinge on logistics. Logistics is the organization of resources to get them to a specific place at a specific time to ensure that the effects of a disruption or loss are minimized (Protiviti, 2010). Assessing resources for the preparedness program starts with reviewing program objectives and performance goals. The top goals that an organization wants to achieve include (FEMA, 2014a):

- Protect the safety of employees, visitors, contractors and others who may be at risk from hazards at the facility
- Maintain customer service by minimizing disruptions of business operations
- Protect facilities, physical assets and electronic information
- Prevent environmental pollution
- Protect the organization's brand, image, and reputation

For each objective, a valuation of resources is needed to achieve the desired results. Simple objectives may require limited resources. Complex objectives will require numerous resources with significant capabilities that can be readily available. It can prove difficult to obtain your desired objectives without adequate resources, or if the

available resources are deficient of the required capabilities. When the organization is identifying certain resources for the preparedness program, the assessment should answer the following questions: (FEMA, 2014a)

- What quantity of a resource is required?
- When will the resource be needed?
- What capability does the resource need to have?
- Are there any limitations?
- What is the cost for procuring or having the resource available?
- Are there any liabilities associated with use of the resource?

Table 2 displays an example of a worksheet that FEMA utilizes to list a company's resource requirements (FEMA, 2014a).

Resource Category	Resource Details	Normal Quantity	Quantity Needed Following Disaster			
			24 hours	72 hours	1 week	Later (specify)
Managers						
Staff	Primary site, relocation site and recovery site					
Office space						
Office equipment	Furniture, phone, fax, copiers					
Office technology	Desktops and laptops (with software), printers with connectivity; wireless devices (with email access)					
Vital records, data, information	Location, backups, and media type					
Production Facilities	Owned, leased, or reciprocal agreement					
Production machinery & Equipment	Especially custom equipment with long replacement time					
Dies, patterns, molds, etc. for machinery & equipment						
Raw Materials	Single or sole source suppliers and possible alternates					
Third party services						

Instructions: Identify resources required to restore business operations following a disaster. Estimate the resources needed in the days and weeks following the disaster. Also review information technology disaster recovery plan for restoration of hardware and software.

Table 2. Business Continuity Resource Requirements (from FEMA, 2014a)

The importance of an emergency response plan is essential to ensure that services are not interrupted for prolonged periods of time. The initial actions that an organization takes at the beginning of the emergency are crucial. A quick caution to employees to evacuate, shelter or lockdown can save lives (FEMA, 2014a). The first step to develop an emergency response plan is to perform a risk assessment to identify emergency scenarios that could possible happen at your organization. This risk assessment should have already been conducted as outlined earlier. Having an understanding of what can occur will enable the organization to control resource requirements and help with the development of plans and procedures to keep the business prepared for any situation that may arise (FEMA, 2014a). This emergency plan should be in line with your performance objectives. Table 3 displays an example of a worksheet that FEMA utilizes to list a company's emergency response resource requirements (FEMA, 2014a).

	Resource Category	Function / Purpose	Quantity	Response Time	Knowledge / Training Capability/Limitations	Cost / Liability	Comments
INTERNAL	Human Resourses (Personnel required if function is performed)	Evacuation Team					
		Shelter-In-Place Team					
		First Aid / CPR Team					
		Hazardous Materials					
		Rescue					
		Supervise Building Systems and Utilities (emergency power HVAC, etc.)					
		Security					
		Property Conservation					
	Systems	Warning System (Fire Alarm, Public Address, tornado siren, etc.)					
		Exits (2 exit routes from all areas, assembly area outsided)					
		Fire Protection (detection, alarm, sprinklers, special supression)					
		Pollution containment					
		Other					
	Equipment	Communications (radios, landline and wireless phones, smartphones)					
		First Aid / Automated External Defibrillator (AED)					
		Fire Protection (fire extinguishers)					
		Spill containment and cleanup					
		Personal protective equipment					
		Tools					
		Other					

Table 3. Emergency Response Resource Requirements (from FEMA, 2014a)

At a minimum, each facility should develop and implement an emergency plan for protecting employees, visitors, contractors and anyone else in the facility. This part of the emergency plan is called "protective actions for life safety" and includes building evacuation ("fire drills"), sheltering from severe weather such as tornadoes, "shelter-in-place" from an exterior airborne hazard such as a chemical release and lockdown. When the facility goes into lockdown, it is important to protect the organization from an act of violence. Life safety should always be the first priority whenever an emergency occurs. The second should be to stabilize the incident before further damage can be done. Details of how to stabilize incidents should be thoroughly explained in the emergency response plan. A plan should be developed to ensure that resources can be readily available to ensure a facility is properly prepared when an emergency occurs. The plan should also include a process for damage assessment, salvage, protection of undamaged property and cleanup following an incident. These actions can be used to minimize further damage and decrease the time that the business or its processes are disrupted (FEMA, 2014a).

Communication is essential when an emergency occurs and it must happen immediately. Once business operations are interrupted, customers want to know how they will be impacted and for how long. Employees and their families will be concerned and they will want information about the current situation. This is why it is important to develop a crisis communications plan as part of the emergency response plan. A business must be able to respond quickly, precisely and confidently during an emergency in the hours and days that follow. Many different audiences must be reached with information specific to their interests and needs. If the incident is not handled properly, there could be positive or negative impacts on the business brought on by public perceptions. The business has to be able to identify potential audiences and determine their need for information and then decide who within the business can best communicate with that audience. The following is a list of potential audiences (FEMA, 2014a):

- Customers
- Survivors impacted by the incident and their families
- Employees and their families
- News media

- Community—especially neighbors living near the facility
- Company management, directors and investors
- Government elected officials, regulators and other authorities
- Suppliers

Another plan that should be created as part of the BCM plan is an information technology disaster recovery plan (IT DRP). Businesses utilize information technology to quickly and effectively process information. It is also used for various means of communication. Electronic data interchange (EDI) is used to transmit data as well as orders and payments from one business to another. Companies use network servers to process information and store huge volumes of data. Desktop computers, laptops and wireless devices are used by employees to create, process, store, and manage data as well as communicate information with other entities and businesses.

An important question has to be answered. What do you do when your information technology stops working? This is why it is important that a business develop an IT DRP in conjunction with a BCM plan.

The business objectives for information technology should be developed during the BIA phase. Technology recovery strategies (previously discussed during this report) should be developed to restore hardware, applications and data in time to meet the needs of the business recovery. Organizations manage large volumes of electronic data that are vital to the survival and continued operation of the business. There could be significant implications if data is lost or corrupted due to hardware failure, human error, and cyber-attacks (FEMA, 2014a). This is why it is essential for a plan to be developed for data backup and restoration of electronic information (Swanson et al., 2010).

After reviewing various resources, it is recommended that the organization's BCM plan focus on the specific content necessary to enable effective response and recovery activities. Most importantly the written strategy should comply with government regulations, which provide specific guidance pertaining to business continuity strategy. Since BC or DR regulations do not apply in all situations, it is imperative that an organization understands the statutes governing data accessibility,

reliability, and compliance prior to developing the BCM plan. Regulations will be briefly discussed in Chapter IV.

This BCM plan should also address the facilities and resources required to enable affected business operations and processes to resume without any further delays. When developing the BCM plan careful attention should be given to using checklists and flow charts to summarize response and recovery procedures. Lastly, an organization should schedule exercises to test the plan and identify areas for improvement (Protiviti, 2013).

E. TESTING, TRAINING AND EXERCISE

In the event of a business disruption, all essential personnel involved in the BCM process should understand their roles and responsibilities. Personnel should regularly rehearse their roles to test the BCP practicality, validate its currency, confirm their competence and confidence and test their assumptions around access to resources (GU, 2013).

BCM training should be mandatory for all personnel. This requires a strict regimen of receiving specific instruction involving actual execution of BCM activities. It is necessary to evaluate the effectiveness or capabilities of the plan and solidifying that instruction with actual proficiency exercises. Key partners and suppliers should also be considered at the appropriate times. This training may be provided through classroom workshops using instruction manuals, computer-based interactive learning, and/or instructional guides and templates or other ad hoc communication methods.

Some organizations utilize BCP testing exercises as a means of training their employees, but beware of the potential pitfalls of doing so. It is not uncommon for testing exercises to reveal discrepancies or weaknesses in the BCP program that need to be addressed. Training should involve the actual execution of business continuity testing activities necessary to evaluate the effectiveness or capabilities of the plan, awareness may be provided through workshops, instruction manuals, email communication or other ad hoc communication methods.

No emergency plan is ever actually finished. The external work environment is constantly changing, and people, methods, tools and systems within your organization change. Therefore, there is no endpoint to the process of training, testing, and revising the plan.

Apply the following concepts in the same priority order—train, test and maintain:

1. The individual readiness plan

2. The emergency action checklist

3. The business continuity plan.

It is insufficient to gather resources and write the plan. If it is to remain functional, it must be continually tested and updated, and if that is to happen, it requires the ongoing support of senior management. Everyone in the workplace must be included in training, and at the appropriate times one may wish to include key partners and suppliers. Simply instructing staff to read the plan is not training, and does not provide the benefits of discussion and practice.

Training can be as simple as a discussion during a regular meeting, or as complex as a full-scale exercise. Training should be planned and scheduled so that staff can methodically move through each major area of the plan. We suggest by appointing someone to develop a training plan for the year. For a 12-month period, determine (CEMA, 2006):

- Who will be trained?
- Who will do the training?
- What training activities will be used?
- When and where sessions will take place?
- How the session will be evaluated and documented?

General training for all employees should address:

- Individual roles and responsibilities
- Information about threats, hazards and protective actions
- Means for locating family members in a crisis

- Office notification, warning and communication systems and procedures
- Proper crisis response procedures
- Location and use of common emergency equipment
- Testing of preparedness strategies and plans

Training can take many forms. There are several levels of training activities you should consider:

- Orientation and education sessions. These are discussion sessions to provide basic information, answer questions and identify needs and concerns.
- Tabletop exercise. A session facilitated by one or more individuals. The staff meets in a conference room setting to discuss their responsibilities and how they would react to various crisis scenarios.
- Walk-through drill. This is a facilitated exercise where all participants actually perform their functions for the given scenario. A walk-through requires more preparation, takes more time and in general is more labor intensive than the previous training methods. They often reveal problems not revealed in simpler forms of training.
- Functional drill. These are targeted drills that are designed to test a specific area of response such as emergency medical response, warning and communications procedures or an evacuation or sheltering problem.
- Full-scale exercise. A real-life emergency situation is simulated as closely as possible. This level of exercise would typically involve not only your staff, but community first-response agencies as well. These are complex drills that take a great deal of planning and coordination among all the internal and external actors.

F. RESOURCES

There are many resources available that can be utilized by the organization to prepare for future disruptive events that can affect business processes. Software is available from vendors for purchase or downloaded at no cost. The Business Continuity Planning Suite is free downloadable software that is highly recommended. This software was created for any business with the need to create, improve, or update its business continuity plan. It was developed by DHS National Protection and Programs Directorate and FEMA for use on personal computers. It is accessible for optimal use by organizations and comprised of a business continuity plan (BCP) training, automated

BCP and disaster recovery plan (DRP) generators, and a self-directed exercise for testing an implemented BCP. Organizations can utilize this software solution to maintain or resume normal operations and provide flexibility during a disruption (FEMA, 2014b).

The BCP training module of the software is a 30 minute video-based course, which examines the importance of BCP, provides a synopsis on business continuity and prepares users to create their own plans. It focuses on three elements of BCP (FEMA, 2014b):

- What is business continuity planning?
- Why is business continuity planning important?
- What is the business continuity planning process?

Upon completion of the training, an organization should possess a rudimentary understanding of BCP, the process of developing and completing a BCP, and the motivation to complete its own plan using the software's BCP generator (FEMA, 2014b).

The BCP and DRP generators were developed to guide businesses through the writing process for continuity plans. They have an overall functionality comparable to automated tax preparation tools. The BCP Generator constructs a plan that guides a company through any disruption to normal business processes or operations, while the DRP Generator focuses on creating a plan specific to recovery of information technology systems. A save and exit option in both generators allows users to complete their plans in increments, and a print option permits users to produce and save hard copies for review (FEMA, 2014b).

The final section of the BCP Suite is a self-directed exercise for testing an implemented BCP and it allows users to test their newly implemented business continuity and disaster recovery plans. This homeland security exercise, evaluation program, and compliant table top exercise centers on a business' recovery efforts following selected business disruptions intended to represent a broad spectrum of threats that include a hurricane, earthquake, ice storm, and blackout. The objective of the exercise is to improve an organization's overall recovery capabilities and actions and the joint decision making process. This process is supposed to lead to an open, stimulating exchange of

philosophies to help develop and expand existing knowledge of policies and procedures within the framework of an organization's BCP implementation.

BCI highly recommends The Good Practice Guidelines (GPG), which is a reliable reference for good business continuity practices globally. The GPG embodies current global philosophy which includes terminology from ISO 22301:2012, the International Standard for business continuity management systems (BCI, 2014b).

The GPG draws upon the extensive academic, technical and practical experiences and aptitude of business continuity professionals from around the BCI's global statutory membership. It also is subjected to a rigorous quality assurance process to ensure it continues to adhere to the highest standards in business continuity practices worldwide (BCI, 2014b).

The true value of the GPG to the business continuity community is that it considers not just the 'what' to do but also the 'why', 'how' and 'when' of common practices used by real-world experts. Although the GPG provides a robust and well proven guide for all participants of business continuity, it also serves as a standard industry benchmark against which all organizations can be effectively measured. This would lead to a thorough examination of an organization's professional and technical capabilities (BCI, 2014b).

There are six practices that are included in the GPG are policy and program management, analysis, design, implementation, validation and embedding business continuity. These six sections comprise the BCM life cycle, which is essential to good business continuity practice and ensures the success of any BCM program and its continued value to the organization (BCI, 2014b).

IV. REGULATIONS

A. OVERVIEW

Regulatory compliance is a significant factor influencing the development of business continuity strategy. While business continuity or disaster recovery regulations may not apply in every business situation, a general understanding of legislation governing data availability, integrity, and compliance is helpful for any organization developing a business continuity strategy. Essentially, there are two specific types of regulations:

- Standards and requirements that must be met in order to become a member of an organization (e.g., International Standardization Organization [ISO]).
- Government regulations (see Table 4), which industries must follow in order to do business. These regulations protect the security of citizens and create national standards of uniformity.

Vin D'Amico (2004) says, according to the Association of Records Managers and Administrators, about 60 percent of businesses that experience a major disaster such as a fire close within two years. The Labor Department statistics showed over 40 percent of all companies that experience a disaster never reopen and more than 25 percent of those that do reopen close within two years.

GOVERNMENT REGULATIONS	IMPACT: BUSINESS CONTINUITY	TAKEAWAYS
Continuity of Operations (COOP) and continuity of Government (COG) Federal Preparedness	Establishes requirements for BC plans and response readiness BC plans must be able to sustain operations for 30 days	All BC plans must be maintained at a high level of readiness, must be capable of implementation without warning, must be operational within 12 hours of activation
FEMA FRPG 01–94	All department and agency heads must formally plan for continuity of essential operations	Written documents for BC must be maintained and current
Federal Information Security Management Act (FISMA) 2002	Requires electronic data to be available during a crisis	Emphasis of FISMA is on data security

GOVERNMENT REGULATIONS	IMPACT: BUSINESS CONTINUITY	TAKEAWAYS
National Institute of Standards and Technology (NIST) SP800-34 2002	Requires electronic data to be available during a crisis	Emphasis of FISMA is on data security
National Institute of Standards and Technology (NIST) SP800-34 2002	Requires BC/DR and COOP plans	
NIST 800–53 2005 Recommended security controls for Federal Information systems	Mandatory security controls that have specific requirements for continuity planning and testing	Specific details on policy and procedures, plans, training, testing, and updating
Governmental Accounting Standards Board (GASB) Statement No. 34 1999	Requires a BC/DR plan to ensure that agency's mission continues in time of crisis	Applies to all government entities that operate utilities

Table 4. List of Government Regulations

B. POLICY

In an effort to enhance the readiness posture, the Deputy Secretary of Defense issued the DOD Directive 3020.26 on January 9, 2009 which outlines the Department of Defense Continuity Program (see Figure 10). It revises continuity policies and assigns responsibilities for developing and maintaining defense continuity programs. This directive applies to all the DOD components. For a compiled list of directives and instructions in related to business continuity and information awareness, see appendix A. The directive defines the following terminologies:

- Continuity of government (COG): A synchronized effort within each branch of government to ensure capability of continuing a minimum of branch-essential responsibilities in a catastrophic crisis. COG relies on effective continuity of operations plans and capabilities.
- Continuity of operations (COOP): The internal effort of each DOD components in ensuring uninterrupted, essential functions across a wide range of possible emergencies— including local acts of nature, accidents, and technological attacks— and related disasters.
- Enduring constitutional government (ECG): A cooperative effort between the executive, legislative, and judicial branches of the federal government, coordinated by the President, to preserve the capability for executing

constitutional responsibilities in catastrophic crises. ECG is the overarching goal; its objective is the preservation of the constitutional framework under which the Nation is governed. ECG relies on effective COOP and COG capabilities.

- Mission essential functions (MEFs): The stated or implied responsibilities performed by or derived from statutes, executive orders, or other appropriate guidance. These organizational activities must be performed under all circumstances to achieve DOD component missions or responsibilities in a business continuity threat or event. Failure to accomplish or sustain these functions would considerably affect the Department of Defense's ability to provide vital services or exercise authority, direction, and control.

4. POLICY. It is DoD policy that:

a. All Defense continuity-related activities, programs, and requirements of the DoD Components, including those related to COOP, COG, and ECG, shall ensure the continuation of current approved DoD and DoD Component MEFs under all circumstances across the spectrum of threats.

b. All DoD continuity planning and programming shall:

(1) Be based on the assumption that no warning of attack or event will be received.

(2) Ensure the performance of MEFs during any emergency for a period of up to 30 days or until normal operations can be resumed. The capability to perform MEFs at alternate sites must be fully operational as soon as possible, but no later than 12 hours after COOP activation.

(3) Be based on risk-management assessments to ensure that appropriate operational readiness decisions consider the probability of an attack or incident and its consequences.

(4) Emphasize the permanent and routine geographic distribution of leadership, staff, and infrastructure in order to increase survivability and maintain uninterrupted capability to accomplish DoD MEFs.

(5) Maximize the use of technological solutions to provide information to leaders and other users, facilitate decision making, maintain situational awareness, and issue orders and direction. Technology, information systems and networks must be interoperable, robust, reliable, and resilient.

(6) Integrate critical infrastructure protection, information assurance, operations security, and defense crisis management requirements, as appropriate.

c. Continuity requirements shall be incorporated into the daily and routine operations of all DoD Components.

d. The continuity program supporting the Secretary of Defense shall include dedicated access to communications capabilities at the Pentagon and alternate operating facilities. This will include availability and redundancy of critical communications capabilities to support alternate facilities and distributed operations. It also shall include dedicated access to mobile communications capabilities during transit between operating locations to ensure the execution of DoD MEFs under all circumstances.

Figure 10. Excerpt from DOD Directive 3020.26, Department of Defense Continuity Program (2009)

V. CONCLUSION

A. FINDINGS

After completing our analysis and comparison with industry standards and case studies, first, we identified the threats to the business process and mitigation strategies. We also identified readiness impacts, key decision, and POA&M to initiate. Second, we formulated a framework that exploited vulnerabilities which would drive a change to the business process. Lastly, as a result of our research and comparison of different business processes used by various organizations in the civilian sector, we discovered that one the most effective step-by-step process that can be applied to the BCM framework is the ten step process.

B. RECOMMENDATIONS

Vin D'Amico, (2004) summarized the steps in surviving a disaster and we linked the Navy business process in an effort to maintain business continuity in the event of a disruption.

The steps that follow are based on three critical elements for creating an effective survival strategy: people, process and technology.

1. People are the single most important aspect of recovering from a disaster. People are the organization's most valuable asset. Reassuring and educating them in advance of an emergency situation is the first critical success factor. By defining how personnel should react to a crisis and providing them information and tools to manage that reaction, the impact will be reduced and streamline the transition to emergency operations.

2. Process is the next major element. There are dozens, hundreds, possibly thousands of business processes that the organization executes daily. Some are mission-critical, some are secondary and the rest are for routine support. Processes need to be defined based on mission criticality and how to keep those processes operating when disaster occurs.

3. Technology not just refers to computers and software. You also need to consider production machinery, network equipment, printers, telephones, fax machines, copiers, etc. Some or all of this technology may be unavailable during a disaster.

Below is a summary of the Ten Steps during Business Recovery, which identifies the critical elements.

People

1. Assemble a multi-disciplined planning team
2. Name a sponsor and a planning team leader
3. Define roles and recovery team participants

Process

4. Catalog your business processes
5. Conduct an impact analysis
6. Assess business recovery options
7. Document and test the BCM plan

Technology

8. Identify critical systems
9. Examine system administration procedures
10. Consider redundancy options

Below is a detailed discussion of the ten steps and their critical elements to help in the development of a BCM.

1. People

When disruptive events occur, all work stops. People typically do not know what to do or how to react. Planning efforts will minimize this behavior. Ultimately, people are the most important factor in recovering from disaster. Therefore, focus on the people factors first.

- Assemble a multi-disciplined planning team who will create the roadmap for managing a disaster or disruption. Identify representatives from all departments who are knowledgeable about the business process. Consider representation from customer service, facilities, finance, human resources, IT or network management, operations, purchasing, sales, security, and/or

systems administration. The idea is to identify a mix of skills within the organization. The team will define business requirements, analyze the business impact of various disaster types, design the survival process, identify members of the recovery team, document the survival plan, and oversee testing of the plan. Make sure there is a good cross-section of roles and levels within the organization. People on the planning team should be intimately familiar with company operations. Management staff alone may not know enough of the details to create a thorough survival roadmap.

- Select an executive-level manager and a planning team leader. This is important! The executive manager must be an active participant in the planning process. The efforts required will span the entire organization and require cooperation from multiple departments. This person must be formally designated and be able to clear roadblocks and resolve issues. The planning team leader is the point person for the BCM process. The team leader must assemble the multi-disciplined planning team and lead them in developing business recovery strategies. This person should be a good leader with enough knowledge of the business to be able to ask the right questions and seek out cost-effective answers.
- Define roles and choose participants for the recovery team. The recovery team is responsible for overseeing execution of the survival plan. Team members coordinate activities and lead the recovery efforts within their respective operational areas. They will choose the personnel who will perform specific activities after any declared disaster. The recovery team leader must be designated with the authority to make quick decisions and draw upon whatever resources are needed. The recovery team may be similar to the planning team.

2. Process

We will turn our attention to business processes. The organization should identify the mission-critical processes that represent the backbone of the business. Each process will need people, technology, and logistics to operate effectively. People needs include specific roles and responsibilities that execute a process. Technology needs include essential hardware and software systems for automating the process. Logistics needs include transportation to and from the disaster site as well as a separate recovery site, if one is included in the plan.

1. Catalog the business processes by conducting an inventory of the process components. Solicit information from process owners and managers in order to define the activities within departments that are most critical to the business. Consider what really matters to the business. Processes that

don't make the inventory list may be vital to the long-term success of the organization but not critical to short-term survival.

2. Conduct a BIA once the major processes are identified. What would be the impact on the business if this process could not be performed for several days? Prioritize the business processes based on the BIA. Use three levels of priority. For example:

   - Processes that need to be resumed within 24 hours to prevent serious business impact, such as loss of revenue or a serious adverse impact to customers.
   - Processes that need to be resumed within 72 hours to maintain near normal operations and adequate levels of quality.
   - Processes that can take more than 72 hours and may not be needed at all unless the disaster is unusually long.

3. Assess business continuity options based on the BIA, consider multiple recovery strategies. Are there manual processing options or possibility of engaging an outside agency (i.e., DISA), to take over some or all operations, establishing a remote, redundant site for mission-critical operations. Also consider using a secondary organization for a certain percentage of your workflow. Workflow sharing could help maintain a level of continuity during disruption. As part of this step, define the specific criteria for declaring a disaster and who is authorized to make the declaration. Create a procedure for determining which business processes are impacted by the disaster. Be ready to act quickly and decisively. If a major disruption occurs, time is your enemy! This gets the team mobilized, minimizes losses and accelerates return to normal operations. This step also requires creating an emergency call list. The person declaring the disaster must notify key personnel who in turn may be asked to notify others. This distributed notification approach enables rapid dissemination of information resulting in rapid emergency response.

4. Document and test the plan that is simple and actionable. Such document will have to evolve over time and should not create a large maintenance task. The plan should be tested at least monthly or annually depending on the needs of the organization. Conduct a mock disaster or create a scenario that will simulate a disruption. Walk through the plan and ensure sure it is still valid. This will help the business evolve and grow. The plan will have to change as well if needed. Process owners may find a need to make arrangements for offsite or third-party support to fully implement the plan. This may take several months requiring some short-term survival procedures while the long-term plan is created. It is necessary to conduct a review of the results of each test to show needed

improvements in the plan to keep the business continuity in the event of a disaster. Also, consider involving multiple employees in any mission-critical process so that lone malicious acts are difficult to accomplish.

3. Technology

Process owners need to understand all the physical assets that support each process. In a disruption, some or all of those assets may be unavailable.

1. Identify critical systems like desktop and server computers. There are also firewalls, routers, switches, printers, scanners, fax machines, copiers, telephones, and so forth. Determine which of these devices are critical to the business. Criticality is measured by the ability to conduct business without that device.

2. Examine system administration procedures by reviewing how major systems are maintained. Simple disruptions can often be avoided by following proper administration procedures. Are computers backed-up regularly? Are the backup media stored locally or offsite? Is antivirus software installed and updated regularly? If paper files are generated, are copies stored locally or offsite? Have the copies been digitized and archived for safety? Can your business operate without them?

3. Consider redundancy options by duplicating or mirroring critical systems. This can be done onsite and/or offsite depending on the needs of the business. The subject of "failover" (switching to a redundant system when the primary system fails) is complex and the solutions can be very expensive. For NAVSUP business systems (i.e., ERP which is a 24x7 operation), redundancy is essential.

4. EXPLORE, PLAN, EXECUTE, VERIFY.

Finally, when the BCM framework is completed, the organization will be prepared to tackle any severe disruption to the business with confidence. This means that all the options are explored, planned for the worst case scenarios, executed a test and verified the results. The enterprise is ready!

Technology is a valuable asset to your business. Make sure you're in control of it at all times. Don't let a disaster take your business down with it! (D'Amico, 2004).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

1. List of Department of Defense Directives on Defense Continuity Programs

- DOD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
- National Communications System Directive 3–10, "Telecommunications Operations," July 25, 2007
- National Security Presidential Directive-51/Homeland Security Presidential Directive-20, "National Continuity Policy," May 9, 2007
- "National Continuity Policy Implementation Plan," August 2007
- Section 2674 of Title 10, United States Code, Operation and Control of Pentagon Reservation and Defense Facilities in National Capital Region

2. List of Department of Defense Instructions on Information Assurance (IA) Implementation

- DOD 5025.1-M, "DOD Directives System Procedures," March 5, 2003
- DOD Directive 8000.1, "Management of DOD Information Resources and Information Technology," February 27, 2002
- DOD Directive 8500.1, "Information Assurance," October 24, 2002
- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

ASIS International. (2005). *Commission on guidelines, business continuity guideline: A practical approach for emergency preparedness, crisis management, and disaster recovery.* Retrieved from https://www.asisonline.org/Standards-Guidelines/Guidelines/published/Pages/Business-Continuity-Guideline_A-Practical-Approach-for-Emergency-Preparedness_Crisis-Management_and-Disaster-Recovery.aspx

Business Continuity Institute. (2014a).What is BC? Retrieved from http://thebci.org/index.php/resources/what-is-business-continuity

Business Continuity Institute. (2014b). The good practice guidelines. Retrieved from http://thebci.org/index.php/resources/the-good-practice-guidelines

Chamber of Commerce of the United States of America. (2005*). Business continuity guideline: A practical approach for emergency preparedness, crisis management, and disaster recovery*. Retrieved from https://www.uschamber.com/sites/default/files/legacy/issues/defense/files/guidelinesbc.pdf

Comprehensive Emergency Management Associates. (2006). *Business continuity plan template for United Way North Carolina*. Retrieved from http://www.unitedwaync.org/sites/unitedwaync.org/files/filedepot/D.2%20%20-%20%20Business%20Continuity%20Plan%20Document.doc

D'Amico, V. (2005). 10 Steps for surviving disaster. Handbook of business strategy. Retrieved from http://www.damicon.com/resources/Disaster_Survival.pdf

Defense Information Systems Agency (2014). Continuity of operations/service continuity. Defense Information Systems Agency/Department of Defense. Retrieved from http://www.disa.mil/Services/Computing/Server-Hosting-and-Virtualization/Service-Continuity

Department of Homeland Security. (2011). *Strategic national risk assessment*. Retrieved from http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk- assessment-ppd8.pdf

Department of Homeland Security. (2013). *National infrastructure protection plan partnering for critical infrastructure security and resilience.* Retrieved from http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

Disaster Recovery Institute International (2014). D*isaster recovery institute resources for professional practices*. Retrieved from https://www.drii.org/certification/professionalprac.php?lang=EN

Federal Emergency Management Agency. (2014a). Business continuity plan implementation. Retrieved from http://www.ready.gov/business/implementation/continuity

Federal Emergency Management Agency. (2014b). Business continuity-planning suite. Retrieved from http://www.ready.gov/business-continuity-planning-suite

Federal Emergency Management Agency. (2014c). Business continuity plan testimonials. Retrieved from http://www.ready.gov/business/business-testimonials

Griffith University. (2013). Business *Continuity Management Framework*. Queensland, Australia. Retrieved from http://policies.griffith.edu.au/pdf/ Business Continuity Management Framework.pdf

Hynosky, J. (2010). Naval Supply Systems Command (NAVSUP), Weapon Systems Support (WSS) Allowancing power point presentation. Power point received from NAVSUP POC Timothy Nellet.

Krause, J. (2010.) *Allowance 101 primer. Naval Supply Systems Command, Weapon Systems Support*. power point presentation. Power point received from NAVSUP BSC POC CDR Brett Sullivan.

Logistics Support Incorporated. (2014). Project highlights. Naval Inventory Control Point – Mechanicsburg Reengineered Maritime Allowance Development. Retrieved from http://www.logsup.com/our-experience/recent-project-highlights/

Naval Supply Systems Command (2008). Re-Engineered Maritime Allowance Development system for interns power point presentation. Document received from NAVSUP BSC POC CDR Brett Sullivan.

Naval Supply Systems Command. (2011a). Business continuity management, the process approach. NAVSUP Business Center. Document received from NAVSUP BSC POC CDR Brett Sullivan.

Naval Supply Systems Command. (2011b). *Sustainment through continuity management*. Washington, DC: Naval Supply Systems Command. Document received from NAVSUP BSC POC CDR Brett Sullivan.

Naval Supply Systems Command. (2012). Re-Engineered Maritime Allowance Development system contingency plan. Document received from NAVSUP HQ POC Timothy Nellett.

Protiviti. (2010). Guide to business continuity management, frequently asked questions. Retrieved from http://www.protiviti.com/en-US/Pages/default.aspx

Shaw, G. (2004), The competencies required for executive level business crisis and continuity managers. PhD. Dissertation. Retrieved from http://www.gwu.edu/~icdrm/publications/PDF/Dissertation_Shaw.pdf

Swanson, M., Bowen, P., Phillips, A.W., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems*. NIST Special Publication 800–34 Rev. 1. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California