MISSION ASSURANCE: A REVIEW OF CONTINUITY OF OPERATIONS GUIDANCE FOR APPLICATION TO CYBER INCIDENT MISSION IMPACT ASSESSMENT (CIMIA)

THESIS

Brian L. Hale, Chief Master Sergeant, USAF

AFIT/GIR/ENV/10-J01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/10-J01

MISSION ASSURANCE: A REVIEW OF CONTINUITY OF OPERATIONS GUIDANCE FOR APPLICATION TO CYBER INCIDENT MISSION IMPACT ASSESSMENT (CIMIA)

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Brian L. Hale, BS

Chief Master Sergeant, USAF

June 2010

AFIT/GIR/ENV/10-J01

MISSION ASSURANCE: A REVIEW OF CONTINUITY OF OPERATIONS GUIDANCE FOR APPLICATION TO CYBER INCIDENT MISSION IMPACT ASSESSMENT (CIMIA)

Brian L. Hale, BS
Chief Master Sergeant, USAF

Approved:

Michael R. Grimaila, PhD, CISM, CISSP (Chairman)
9 JUN 2010
Date

Robert F. Mills, PhD (Member)
9 JUN 2010
Date

Michael W. Haas, PhD (Member)
9June 2010
Date

AFIT/GIR/ENV/10-J01

Abstract

Military organizations have embedded information technology (IT) into their core mission processes as a means to increase operational efficiency, improve decision-making quality, and shorten the sensor-to-shooter cycle. This IT-to-mission dependence can place the organizational mission at risk when an information incident (e.g., the loss or manipulation of a critical information resource) occurs. Non-military organizations typically address this type of IT risk through an introspective, enterprise-wide focused risk management program that continuously identifies, prioritizes, and documents risks so an economical set of control measures (e.g., people, processes, technology) can be selected to mitigate the risks to an acceptable level. The explicit valuation of information resources in terms of their ability to support the organizational mission objectives provides transparency and enables the creation of a continuity of operations plan and an incident recovery plan. While this type of planning has proven successful in static environments, military missions often involve dynamically changing, time-sensitive, complex, coordinated operations involving multiple organizational entities. As a consequence, risk mitigation efforts tend to be localized to each organizational entity making the enterprise-wide risk management approach to mission assurance infeasible.

This thesis investigates the concept of mission assurance and presents a content analysis of existing continuity of operations elements within military and non-military guidance to assess the current policy landscape to highlight best practices and identify policy gaps in an effort to further enhance mission assurance by improving the timeliness and relevance of notification following an information incident.

AFIT/GIR/ENV/10-J01

In loving memory of my wonderful wife.

Acknowledgments

I would like to express my sincerest appreciation to my research advisor, Dr. Michael R. Grimaila, for his guidance and untiring support throughout the course of my thesis effort. His patience in working with me and his enthusiasm in support of this stream of research were unequaled. Furthermore, Dr. Grimaila's insights, experience, and counsel were immensely valued. I would also like to thank my thesis committee, Dr. Robert F. Mills and Dr. Michael W. Haas, for their contributions in directing my research.

Additionally, I would like to thank my family and friends for their unconditional love and continuous support. Their encouragement is always inspiring. Finally, I would like to especially thank my daughter for her love and providing me the motivation to persevere through life's challenges.

Brian L. Hale

Table of Contents

Page

List of Figures

Page

List of Tables

Page

MISSION ASSURANCE: A REVIEW OF CONTINUITY OF OPERATIONS GUIDANCE FOR APPLICATION TO CYBER INCIDENT MISSION IMPACT ASSESSMENT (CIMIA)

I. Introduction

"When the well's dry, we know the worth of water."

- Benjamin Franklin

Background

Information has become the critical asset in the operation and management of virtually all modern organizations (Abrams, Jajodia, & Podell, 1995; Davenport & Prusak, 2000; Denning, 1999; Department of the Air Force, 2006a; National Institute of Standards and Technology [NIST], 2008c; Pipkin, 2000). Organizations continue to embed information technology (IT) into their core mission processes as a means to increase their operational efficiency, exploit automation, reduce response times, improve decision quality, minimize costs, and/or maximize investments (Alberts, 2002; Alberts, Garstka, & Stein, 1999; Department of Defense [DoD], 2009b; Rubin, 2010). This is especially true in military environments where information is constantly being collected, processed, analyzed, distributed, and aggregated to support situational awareness, operations planning, intelligence, and command decision making (DoD, 2006b). However, the increasing dependence upon information and IT to produce value within the organization has resulted in an environment where an information incident (e.g., the loss or degradation of the confidentiality, availability, integrity, non-repudiation, and/or authenticity of an information resource or information flow) can result in significant mission degradation or failure (Anderson, Choobineh, & Grimaila, 2005; Fortson & Grimaila, 2007; GAO, 1996; Grimaila & Fortson, 2007; Jajodia, Ammann & McCollum, 1999; Ware, 1970). When this incident occurs, the decision makers within organizations whose mission is critically dependent upon the affected information must be notified in a timely manner so they may take appropriate contingency actions.

Organizations typically employ an enterprise-wide focused risk management program that identifies and prioritizes risks so a set of control measures (e.g., people, processes, technology) can be selected to mitigate the risks to an acceptable level given a limited budget (COBIT, 2007; COSO, 2004; I^{2}SF, 2005; (ISC)^2, 2009; ISSA, 2005; NIST, 2002; OCTAVE, 2004; Petrocelli, 2005). Risk management has proven successful in static environments, when all stakeholders participate, and all resources critical to the success of the operations can be enumerated. However, military missions often involve dynamically changing, distributed, time-sensitive, complex, cooperative, and coordinated operations involving multiple organizational units within a military service (e.g., fighter squadrons, aerial refueling squadrons, special operations units), between various service elements (e.g., Army, Navy, Air Force, Marines), between various national agencies, and across multiple allied coalition partners (Alberts & Hayes, 2006). Because each organization participating in the mission is resourced and managed as a separate entity, a centralized enterprise-wide risk management approach is largely infeasible. Since the accuracy, conciseness, and timeliness of the information used in decision-making processes dramatically impacts the quality of command decisions, and hence the operational mission outcome, the recognition, quantification, and documentation of critical information dependencies is essential for the organization to gain a true appreciation of its operational risk (DoD, 2010; Grimaila, Fortson, & Sutton, 2009; Quadrennial Defense Review [QDR], 2010). By explicitly documenting information dependencies and formalizing the linkage between mission operations and the underlying dependent information resources, mission commanders and their staff can maintain awareness of their critical information resources during mission operations and ultimately, improve situational awareness. When an information incident occurs, the incident notification can recall and display context-dependent information collected when documenting the linkage between information dependencies and mission operations, to include potential contingency measures.

Problem Statement

Non-military organizations that conduct risk management are better prepared to deal with, and recover from, the impacts to their mission objectives resulting from information incidents. For example, after the September 11, 2001, attack on the World Trade Center, the financial firms of Lehman Brothers and Cantor Fitzgerld were able to quickly resume operations because they had established backup data facilities as an element of their business continuity contingency plans (Moss & Townsend, 2004). The complexity and distributed workflow process of organizations makes the adoption of risk management and assessment extremely challenging (Alberts & Dorofee, 2005). The nature of this new organizational environment extends to the dynamic and decentralized nature of military operations and has prevented the direct adoption of a standardized, centralized risk management process.

This thesis seeks to improve mission assurance by developing a clear understanding of the concept of mission and mission assurance and by conducting a content analysis of existing continuity of operations components within military and non-military guidance, advance one aspect of mission assurance: improving the timeliness and relevance of notification following a cyber incident.

Research Questions

This research strives to answer the following research questions in order to advance mission assurance through improving the timeliness and relevance of cyber incident notifications:

RQ1. What is mission?

RQ2. What is mission assurance?

RQ3. What are risk management and risk assessment, and how are they used to support mission assurance?

RQ4. How are risk management and risk assessment conducted in military and non-military environments?

RQ5. What elements of continuity of operations are required to enable mission assurance?

RQ6. How are mission impacts represented through risk management and risk assessment to facilitate continuity of operations planning?

Research Scope

Prior research and the perspective of this follow-on research are from the context of military operations, although non-governmental guidance is also examined to extend any applicable findings and best practices to military operations. This research continues within the Cyber Incident Mission Impact Assessment (CIMIA) stream of research (Table 1).

Table 1. Summary of CIMIA-Related AFIT Thesis Research

Research	Author
Mission Impact/Visualization	
Enabling Network Centric Warfare Through Operational Impact Analysis Automation ▪ Mission impact analysis of link state availability	Stanley, 2005
Graph Theoretical Analysis of Network Centric Operations Using Multi-Layer Models ▪ Proposed to extend Network Centric Operation (NCO) Common Framework ▪ NCO model for holistic view of mission dependencies between entities	Wong-Jiru, 2006
A Model for Performing Mission Impact Analysis of Network Outages ▪ Proposed model of network outages ▪ Modeled Air Tasking Order process at Combined Air And Space Operations Center with the goal to prove mission database feasibility, tied to mission essential task lists	Shaw, 2007
Mission Impact Analysis Visualization for Enhanced Situational Awareness ▪ Examined creation of mission impact analysis visualization to enhance situational awareness; allow decision makers to understand the scope of mission impact when network outages occur	Carroll, 2008
Developing Network Situational Awareness through Visualizations of Fused Intrusion Detection System Alerts ▪ Examined theory, application, and results of using visualizations of fused alert data to develop network situational awareness	Avitia, 2008
Damage Assessment	
A Study to Determine Damage Assessment Methods or Models on Air Force Networks ▪ Highlighted lack of standardized network damage assessments	Thiem, 2005
Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology ▪ Proposed operations-focused defensive cyber damage assessment and mission impact methodology	Fortson, 2007
System Design	
A System Architecture for Cyber Incident Mission Impact Assessment (CIMIA) ▪ Proposed a system architecture for Cyber Incident Mission Impact Assessment	Sorrels, 2008
Integration of Cyber Situational Awareness Into System Design and Development ▪ Recommended improvements to acquisition policy and guidance, advocating cyber issues be an integral part of early system design and development	Chase, 2009
Information Asset Valuation	
An Analysis of Information Asset Valuation Qualification Methodology for Application with CIMIA ▪ Proposed an information asset valuation schema	Hellesen, 2008

The purpose of CIMIA research is to develop a structured process to provide decision makers with timely notification and relevant estimation of mission impact, from the time an information incident is declared, until the incident is fully resolved, so decision makers can take appropriate contingency measures (Grimaila et al., 2009).

Specifically, this research attempts to assist in assuring missions and the continuity of operations by investigating current government and non-government mission assurance, continuity planning, risk management, and incident management policies and analyzing the guidance for application towards improving the timely and relevant notification of decision makers following an information incident.

Research Significance

In 1996, eight national critical infrastructures were specified in Presidential Executive Order 13010 as being so vital that their "incapacity or destruction would have a debilitating impact on the defense or economic security of the United States" (p. 1). One of the centers of gravity included was the continuity of government. The threats to the critical infrastructures were classified into two categories: physical and cyber threats (Executive Order No. 13010, 1996).

Cyber threats continue to escalate and cyberspace has grown to be a contested domain (Baker, Waterman, & Ivanov, 2009). Simultaneously, the mission dependency on cyber assets continue to rise (Lyle, 2009; Millette, 2010). Coupling the expanding threats and cyber dependencies increases the potential for cyber-related risks to potentially disrupt operations. The recently declassified 2010 Comprehensive National Cybersecurity Initiative (CNCI) identifies cybersecurity as one of the most serious economic and national security challenges the United States faces, and that the nation is inadequately prepared to deal with these challenges (CNCI, 2010). The acknowledged importance of mission to cyberspace dependency is further identified in the United States Air Force Blueprint for Cyberspace. One of the objectives stated in the blueprint is "to ensure mission success by maximizing cyber continuity, availability, and resilience" (Air Force Space Command, 2009, p. 11). This speaks to the seriousness and noted contested nature of cyberspace. However, initiatives such as improved cyberspace situational awareness, security, and information assurance efforts across the cyber infrastructure may elevate resiliency and improve operational capabilities.

To ensure Defense Critical Infrastructure (DCI) availability, the DoD uses the DCI Program (DCIP), a risk management program (DoD, 2008). It is DoD policy to conduct assessments of the threats and hazards, vulnerability, and risk to DoD-owned DCI and the inter- and intra-dependencies needed to accomplish required DoD missions, with the support of the appropriate DoD Components and Defense Infrastructure Sector Lead Agents. These activities are the major elements of the DCIP and the actions should support incident management. Also, the DCIP must coequally complement other DoD programs, functions, and activities contributing to mission assurance through risk management (DoD, 2010).

The 2010 Quadrennial Defense Review (QDR) report further recognized risk management as central to effective decision-making and is vital to mission success, although it can be challenging to accomplish. The QDR noted the need for non-quantitative methods (informed judgments, expert opinions, scenarios) to improve the military complexity associated with the identification, categorization, and aggregation of operational risk (QDR, 2010).

Recognizing the increasingly contested nature of cyberspace, the need to enhance awareness of cyber dependencies, and the need for non-quantitative risk assessment measures, the research presented in this thesis seeks to enhance mission assurance by surveying mission assurance, continuity planning, risk management, and incident management policies and guidance, and analyzing the results for application towards improving the timely and relevant notification of decision makers following an information incident.

Thesis Structure

This thesis includes five chapters and supporting information found in the appendices. This chapter provided an introduction, an overview to the research questions, and the motivation to complete the research. Chapter 2 provides a more detailed review of the existing literature and reviews the concepts and definitions of mission, mission assurance, risk management, risk assessment, continuity of operations planning, and contingency planning in order to provide the background necessary to identify key terms and concepts used in the content analysis. Chapter 3 discusses the content analysis research methodology and explains how this research was designed. Chapter 4 presents and analyzes the results of the content analysis. Chapter 5 includes further discussion and recommendations, along with research limitations and future research ideas. Readers can find additional supporting information for this research in the back of this report under the appendices, bibliography, and researcher’s vita.

II. Literature Review

"Don't be afraid to see what you see."

- President Ronald Reagan

Introduction

In this chapter, a literature review is presented containing topics relevant to this research effort. Specifically, this chapter discusses aspects of mission, mission assurance, risk management, risk assessment, continuity of operations, and contingency planning that are relevant to address the stated research problems.

Mission

Military missions often involve dynamically changing, time-sensitive, coordinated operations involving multiple organizations. As such, missions are often complex. This complexity seems to extend to the definition of mission as the term is not necessarily well defined across the defense community (Donley, 1995). The term "mission" is frequently written in publications; but, mission is rarely defined within the same publications. For example, this is evidenced in the publication that prescribes and describes Air Force Mission Directives (AFMD), Air Force Instruction (AFI) 10-101, *Format and Content of Mission Directives*, 2003. AFMDs provide guidance about an organization's mission and describes what an organization does (Department of the Air Force, 2003). However, mission is not defined within the instruction itself. The assumed meaning of mission and the complexity of missions causes confusion about the term (Alberts & Dorofee, 2005).

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 2001, defined mission as:

> 1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.
> 2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task.
> 3. The dispatching of one or more aircraft to accomplish one particular task. (p. 349)

Former Assistant Secretary of the Air Force Michael Donley analyzed the use of the term mission in Chairman Joint Chiefs of Staff reports, JP 1-02, and Title 10 of the United States Code and defined missions similar to JP 1-02; however, Donley further stated a mission is “considered generally as integrating many activities around a common theme or purpose” (1995, p. 87). This integration of activities, and usually the combination of organizational entities performing the activities, leads to the complex nature of missions. Nonetheless, the accepted definitions of mission appear to be tasked focused. As specified in Title 10, Chapter 2, of the United States Code, the Secretary of the DoD must include a description of the major military missions to Congress each year. Additionally, it is important to differentiate mission from roles (broad, enduring purposes) and functions (powers, duties, and responsibilities) (Donley, 1995). DoD Directive (DoDD) 5100.01, *Functions of the Department of Defense and Its Major Components,* 2002, prescribes three functions of the DoD.

In the keystone publication for joint operation planning doctrine, missions are linked to tasks through objectives and effects. Three types of tasks are defined: specified, implied, and essential. A specified task is specifically assigned by higher headquarters. An implied task is not directed by higher headquarters; however, an implied task is derived during mission analysis as a task that must performed to accomplish a specified task or the mission. An essential task is either a specified or implied task that must be performed to accomplish the mission (DoD, 2006c). The relationship between missions, operations (military action), and tasks are shown in Figure 1.

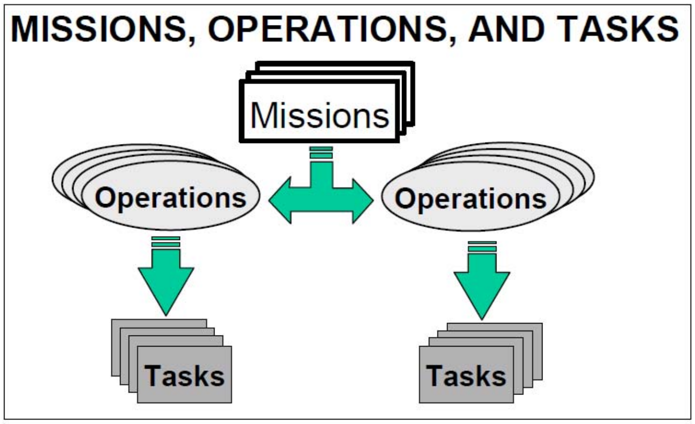

Figure 1. Relationship of Missions, Operations, and Tasks (DoD, 2002c, p. A-8)

To communicate mission requirements, the Universal Joint Task List (UJTL) serves as a common language and reference system to communicate a joint mission essential task list (JMETL) or agency mission essential task list (AMETL). JMETLs are developed to identify the required capabilities for mission success (DoD, 2002c). To further identify Air Force unique tasks, the Air Force Universal Task List (AFUTL) incorporates Air Force-specific tasks and extends the UJTL to show hierarchy. There is an effort underway to further extend the METL construct and create Air Force core unit METLs. The core unit METLs would describe the essential tasks in a unit's mission, would include mission essential tasks from either the UJTL or the AFUTL, and must include specific conditions, measures, and criteria. In effect, this expanded METLs hierarchy would provide the basis for linking capabilities to tasks (AF/A3O, 2008).

Mission Assurance

With a common understanding of mission, and the posited linkage to tasks, what does it mean to assure a mission? DoD Directive 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, 2010, defines mission assurance as:

> A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA; continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. (2010, p. 19)

In this definition, risk management activities are essential to the ability to provide mission assurance through the continuity of operations. Also, although supporting infrastructures are not defined, the association of both physical and cyber infrastructures essential to planning and executing military operations is contained within the definition of the Air Force Critical Infrastructure Program (Department of the Air Force, 2005a).

In a recent draft of cyberspace operations doctrine, a distinct cyberspace mission assurance definition was proposed. Mission assurance (cyberspace) is defined in the draft doctrine document as the "measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities" (Department of the Air

Force, 2010, p. 56). The proposed definition highlights the need for connecting mission dependencies to cyberspace, an identification step needed for risk assessment that is not explicitly defined in general risk management frameworks.

To ensure assigned tasks or duties can be performed as intended to assure the mission, as mission assurance strategy must be employed. Through a risk management program, operational risks may be eliminated or reduced to an acceptable level. However, given the DoD hosts 7 million computers and more than 15,000 area networks, and the DoD networks are probed thousands of times per day with an ever increasing frequency and sophistication (Daniel, 2010), it is likely impossible to reduce all cyber-related risks to zero or an acceptable level (Department of the Air Force, 2005a; NIST, 2009). Rosenzweig (2009) noted even when it is feasible to eliminate risk it may be impractical because the risks are systemic and resistant to traditional cost-benefit analysis. Furthermore, “in a world where the identity of the threat cannot be determined with confidence, mitigation of that threat is problematic” (Rosenzweig, 2009, p. 2).

Acknowledging these challenges, as well as the difficulty of conducting risk management across an enterprise as large and complex as the DoD, a strategy and processes must employed to resolve risks as they happen. Resolving problems as they occur (Figure 2) is a central focus area for CIMIA, specifically the timely and relevant notification on cyber incidents.

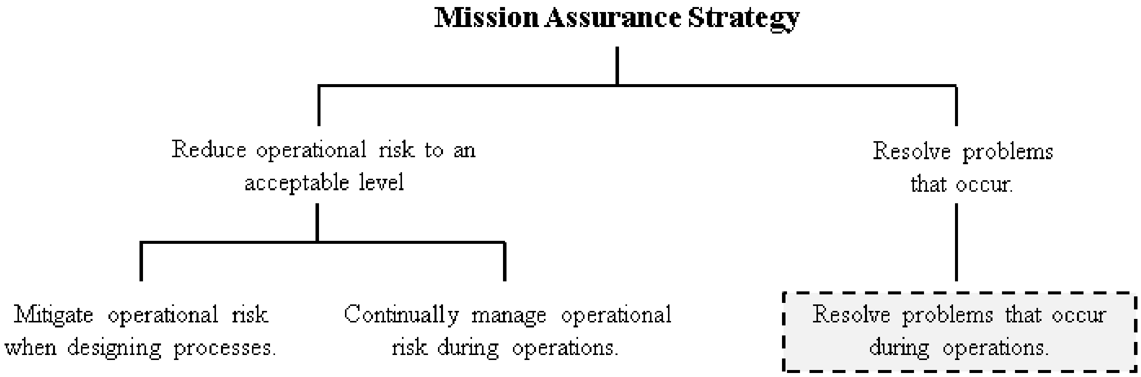
Mission Assurance Strategy
Reduce operational risk to an acceptable level
Resolve problems that occur.
Mitigate operational risk when designing processes.
Continually manage operational risk during operations.
Resolve problems that occur during operations.

Figure 2. Mission Assurance Strategy (Adapted from Alberts & Dorofee, 2005, p. 14)

Mission Assurance: Existing Situational Awareness Tools and Techniques

To help communicate and mitigate problems as they are identified during operations, efforts are reviewed to improve mission assurance by enhancing situational awareness of mission critical resources. The Defense Advanced Research Projects Agency (DARPA) funded research in the area of mission assurance and survivability and their efforts yielded several significant publications related to these objectives (Bickford, Kreitz, van Renesse, & Constable, 2001; D’Amico & Salas, 2003; Goldman, Heimerdinger, Harp, Geib, Thomas, & Carter, 2001; Melliar-Smith, Moser, Kalogeraki, & Narasimhan, 2000; Moore, Kewley, Parks, & Tinnel, 2001; Tinnel, Saydjari, & Haines, 2003). The research focused on defending mission-critical information systems from coordinated attacks through the development of novel sensors, improved methods for alert correlation and reduction, visual attack correlation, and mission impact assessment and response (Tinnel et al., 2003). The mission impact assessment research attempted to formalize the core problem of recognizing critical resource dependencies for the purposes of assurning the mission. Some of the more salient publications are reviewed and a brief commentary on the tool’s strengths and weaknesses is provided.

Secure Scope

D’Amico and Salas (2003) prototyped several mission impact visual displays and incorporated the most promising ones into a visualization software architecture called Secure Scope that can be deployed in an operational setting. The mission impact visualization system was designed to act as a front end to a relational database populated with the resources and tasks required to complete a mission. The tool provided a quick means to visualize impacted resources with a linkage to the tasks affected by an incident. The tool visually represents "bottom-up" mission impact analyses showing the mission effect of a specific breach on a specific asset, as well as "top down" analyses showing cyber assets that must be secured for the achievement of certain mission-critical tasks.

Master Caution Panel (MCP)

The MCP system was developed to provide an improved situational awareness of the potential impacts on the mission operations of an Air Operations Center (AOC) as a function of system and network availability (Jos & Culbertson, 2006). The MCP requires the AOC mission is first decomposed into its’ subordinate mission tasks and the systems and network components that can impact these tasks are explicitly identified. A database is populated with this information and an explicit representation of the relationship between the networking infrastructure components and the operational tasks. The operational tasks are annotated with their percieved criticality and contingency plans are also entered into the system to provide advice to users when a loss of availability of network resource occurs. The database, combined with a network status monitor, provides the ability to present enhanced situational awareness to users within the AOC. The MCP provided great value to the operational community because it enabled the monitoring of mission critical tasks as a function of the status of the availability of the underlying systems and networks on which it depended. In 2004, the MCP was incorporated as a third party enhancement to the Theater Battle Management Core System baseline. However, implementing MCP still required custom programming and worked only on traditional IP networks. The tool also requires manual decomposition of the mission tasks and manual identification of the underlying dependent systems and networks. Finally, MCP focuses only on resources within the AOC and requires a centralized representation of all of the organizations functions within a single server.

Command and Control Resource Management System (C2RMS)

Following the success of MCP, it was clear that a next generation of situational awareness systems needed to be developed to overcome some of the barriers identified in deployment of the MCP. Specifically, C2RMS extended the MCP by providing more flexible and extendable monitoring capabilities, expanding to next generation protocols such as those found in airborne networks, and providing a Monitor Development Kit (MDK) which greatly simplified deployment and customization of instances of C2RMS. This enabled virtually anyone to instrument their organization with the monitiors necessary to collect status from local and remote network resources and to create tailored displays which fuse information from multiple resources. Jos and Cubertson (2006) provided an example which demonstrates the value to commanders when fusing information from multiple sources, including environmental information such as current weather, in a centralized situational view which portrayed the readiness and capability of the aircraft fleet. While the mission tasks and underlying resources still had to be manually identified, the burden of creating monitoring agents and user interface capabilities were greatly reduced by the development of the MDK. Further, multiple instances of C2RMS could be created and communication capabilities were provided to allow communication between these instances to improve situational awareness.

Mission Service Automation Architecture (MSAA)

Stanley, Mills, Raines, and Baldwin (2005) introduced the MSAA. The architecture correlates information flows to operational capabilities providing the ability to prioritize network traffic. MSAA incorporates the concept of IT service codes as defined in the Information Technology Infrastructure Library (ITIL) as a means to align IT services with customer mission requirements. The MSAA requires a configuration management database and collection of independent software agents to provide an understanding of the purpose of information flows. Data tagging is used to provide the needed visibility by inserting IT service management codes into the headers of network packets. When an operational unit requires network services, the network operations personnel are tasked with assigning a unique service code to the requirement and populating the configuration management database with a listing of all of the resources needed to fullfill the requirements and the operational mission processes or capabilities supported. In aggregate, this information can be viewed as a Service Level Agreement

(SLA) between the operational organization and the network personnel. A key benefit of the MSAA is that it allows network operations personnel to quickly identify the impact resulting from network traffic that is delayed or degraded following an network outage. While MSAA has not been operationalized yet, it is clear tagging information flows with service codes would enable network personnel to quickly identify the organizations that are impacted when a network outage occurs and provdes the ability to easily visualize the importance of bulk network traffic. However, MSAA places a burden on network operations personnel to identify the operational mission processes supported in the SLA, requires manual identfiication of the underlying dependent systems and networks, requires a centralized representation of all of the organizations functions within a single server, and is susceptable to adversaries gaining an understanding the criticiality of network flows over time because it encodes service codes into the network traffic.

Camus: Automatically Mapping Cyber Assets to Missions and Users

Most recently, Goodall, D’Amico, and Kopylec (2009) provides further, potential advancement to cyber situational management thorough a proposed method for automated mapping of Cyber Assets to Missions and Users (Camus). The researchers developed methods for aggregating data from multiple, common network feeds, coupled with an ontology-based system to populate a model. This method allows the system to map cyber assets to the users who rely on the assets, to the mission the assets support, and to the services they provide. Additionally, the Campus approach may assist in collecting and automating information assets, going beyond just cyber hardware monitoring.

Risk Management

Before discussing risk management and risk assessment, a clear understanding of the term risk is required. Risk is defined in JP 1-02 as the "probability and severity of loss linked to hazards" (DoD, 2001, p. 470). By international standards, risk is parsimoniously defined as an "effect of uncertainty on objectives" (ISO, 2009b, p. 1). In the 2010 QDR, four risk categories are established and have been used since 2001: operational risk (ability to execute strategy); force management risk (ability to recruit, retain, train, educate, and equip the force); institutional risk (capacity of management and business practices); and future challenges risk (capacity to execute future missions).

A general expression of risk is a function of probability, severity, and exposure, and may be written as: risk = f(P, S, E) (Department of the Air Force, 2000b). However, for information security risks, probability is a more complex and imprecise variable than is normally found in other risk management domains. Because risk factors are constantly changing, probability is highly subjective in the absence of objective data (OCTAVE, 2004). A subjective view of probability can refine the understanding of threat by focusing on information about motives, means, opportunities, historical data, and any unusual conditions of risk (i.e., non-quantitative assessments) to bear on risk management decisions, in support of the 2010 QDR to find qualitative means to improve the military complexity associated with the identification, categorization, and aggregation of risk.

Managing risk includes the process of coordinated activities (identifying, assessing) to direct and control risks (DoD, 2001; ISO, 2009b). DoD extends the definition and stated the process should incorporate a cost/mission benefit assessment

(DoD, 2001). Risk management therefore provides a documented, structured, and transparent process to identify and mitigate risks (Gerber & von Solms, 2005).

Since all activities involve risk and organizations manage risk to some degree, ISO 31000, *Risk management — Principles and guidelines,* 2009, established 11 principles to be satisfied to make risk management effective; the principles are:

> Risk management…
>
> - creates and protects value
> - is an integral part of all organizational processes
> - is part of decision making
> - explicitly addresses uncertainty
> - is systematic, structured and timely
> - is based on the best available information
> - is tailored
> - takes human and cultural factors into account
> - is transparent and inclusive
> - is dynamic, iterative and responsive to change
> - facilitates continual improvement of the organization. (pp. 7-8)

These principles support an overall risk management framework. The purpose of a framework is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values, and culture (ISO, 2009a). A risk management process then operates within the construct of the risk management framework. In ISO 31000 (2009), the fundamental elements of the risk management process are stated as: communication and consultation; establishing the context (determination of risk assessment objectives and risk criteria); risk assessment (comprising of risk identification, risk analysis and risk evaluation); risk treatment; and monitoring and review.

In the context of infrastructure risk, the Defense Critical Infrastructure (DCI) Program supports a risk management process that seeks to ensure DCI availability. DCI availability focuses on defense critical assets.   The DCI Program risk management process is comprised of a risk assessment component that identifies critical assets and infrastructure interdependencies supporting DoD missions. To complete the risk assessment, applicable follow-on threat and vulnerability assessments are conducted on the applicable critical assets. When properly executed, the implemented risk assessment procedures of critical assets enable informed risk management decisions, leading to an appropriate risk response. The risk response component ensures limited resources are optimally allocated toward those assets deemed important to overall mission success. These activities comprise the major elements of DCIP risk management (DoD, 2008).

Specific to information systems, the DoD Information Assurance Certification and Accreditation Process is the DoD process to ensure risk management is applied to information systems (DoD, 2007). However, NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, recognized “the principal goal of the risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets” (NIST, 2002).

Additionally, the Air Force’s effort to institutionalize risk management is through the concept of Operational Risk Management (ORM). ORM is a six-step process of identifying hazards, assessing risk, analyzing risk control options and measures, making control decisions, implementing risk controls, and supervising/reviewing the activity (Department of the Air Force, 2000a). ORM information and training may be located on the Risk Management Information System web site (https://rmis.kirtland.af.mil/default.asp) hosted by the Air Force Safety Center, Kirtland Air Force Base. The site also includes the Total Risk Assessment and Control System, a tool designed to help users apply ORM to assess and control risks affecting missions, operations, systems, and decisions (Air Force Safety Center, 2005).

Risk Assessment

Risk assessment is generically the process of identifying, characterizing, and understanding risk. The roots of modern risk assessment can be traced to the nuclear power industry, where risk assessment methodologies were developed to analyze the operations of the new nuclear power facilities. These methodologies centered on fault/event trees used to capture all possible plant failure modes and display them visually (Soo Hoo, 2000).

The DoD defines risk assessment simply as the identification and assessment of hazards, the first two steps of the DoD risk management process (DoD, 2001). Similarly, the international standards community defines risk assessment as the process of risk identification (finding, recognizing, and describing risk), risk analysis (comprehending nature of risk and to determining level of risk), and risk evaluation (analyzing result of risk analysis with risk criteria (ISO, 2009b).

A general international standard on the selection and application of techniques for risk assessments was published in support of ISO 31000 (risk management). The standard, IEC/ISO 31010, is general in nature and, as such, provided guidance applicable to many types of industries and systems. Of particular interest in this standard is the information provided on 31 tools and techniques used for risk assessment. The standard provided the following detailed information for each of the risk assessment techniques featured: overview, use, inputs, process, outputs, strengths, and limitations (IEC/ISO, 2009).

In respect to system security management, two ISO documents are noteworthy. ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*, 2005, identified the requirements for an Information Security Management System (ISMS). The ISMS is based on an operational risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management,* 2005, specified control objectives (what is to be achieved) and controls (applied to the control objective) intended to be implemented to meet the requirements identified by a risk assessment.

In concert with vulnerability and threat information, security categories are also used in assessing the risk to an organization (NIST, 2004b). Security categories have been established for information and information systems in FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004. The three security categories are: confidentiality (preventing unauthorized disclosure of information), integrity (preventing unauthorized modification or destruction of information), and availability (preventing disruption of access to or use of information). Non-repudiation and authenticity are included as elements of integrity (NIST, 2004b). Furthermore, NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, 2002, described the impacts of the loss of confidentiality, integrity, or availability. For example, the loss of confidentiality could result in the “loss of public confidence, embarrassment, or legal action against the organization” (NIST, 2002, p. 22).

In addition to the categories of confidentiality, integrity, and availability, Parker (2007) posited an additional category described as “Other harmful actions” (p. 5). Included in this category are actions such as: failure to support security, annoy, and waste time or effort (Parker, 2007).

Continuity of Operations

At least since the Cold War era, government organizations have had a requirement to continuously conduct their operations, regardless of any disruptions the organizations may face. However, recent events such as the terrorist attacks of 11 September 2001 against the United States and the cyber attacks against Estonia have reemphasized the need to ensure continuity of operations after a disaster or extended disruption. All organizations should be prepared to respond to a wide range of potential emergencies.

At the national level, Homeland Security Presidential Directive-20, *National Continuity Policy*, 2007, established a comprehensive national policy on the continuity of Federal Government structures and operations. In the directive, the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT) was designated as the National Continuity Coordinator. It is the policy of the United States to maintain a comprehensive and effective continuity capability, consisting of Continuity of Operations and Continuity of Government programs (Homeland Security, 2008).

Within the DoD, continuity of operations (COOP) is defined as:

> The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander. (DoD, 2001, p. 118)

DoD documents also described continuity of government (COG) similarly, with the emphasis on the capability to continue minimum essential responsibilities (DoD, 2009a). The DoD mandated the following COOP guidance (DoD, 2009a):

- Components ensure continuation of current approved DoD and DoD Component mission essential functions under all circumstances across the spectrum of threats
- Continuity requirements shall be incorporated into the daily and routine operations of all DoD Components
- DoD continuity planning and programming must:
    - Be based on the assumption no warning of attack or event will be received
    - Ensure the performance of MEFs during any emergency for a period of up to 30 days or until normal operations can be resumed
    - Be based on risk-management assessments to ensure that appropriate operational readiness decisions consider the probability of an attack or incident and its consequences
    - Emphasize the permanent and routine geographic distribution of leadership, staff, and infrastructure
    - 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

- Integrate critical infrastructure protection, information assurance, operations security, and defense crisis management requirements, as appropriate

Cerullo and Cerullo (2004) recommended the business continuity planning process should address three objectives: identifying major risks, developing a plan to mitigate or reduce the impact of the risks, and testing the plan for effectiveness. In comparison, Air Force guidance mandated the following minimal continuity of operations program elements:

- Program guidance
- Planning and procedures, to include essential functions, delegation of authority, orders of succession, alternate operating facilities, interoperable communications, vital records and databases, and human capital
- Test, training and exercises to assess and validate plans, policies, procedures
- Designation of an organization as the office of primary responsibility and appoint a continuity planning officer (Department of the Air Force, 2005a)

The key elements necessary to maintain continuity and enhance decision-making are command and control, through the organization of appropriate personnel, communication and computers, and information. (Department of the Air Force, 2005a)

Contingency Planning

At the strategic level, contingency planning is used to develop operations plans for a broad range of contingencies. The planning is based on requirements in the

Contingency Planning Guidance (CPG). The CPG fulfills the statutory requirement of the Secretary of Defense to publish policy annually to the Chairman of the Joint Chiefs of Staff for contingency planning. The CPG focuses the guidance given in the National Security Strategy and Defense Planning Guidance (DoD, 2001). A contingency is defined as "a situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect US interests" (DoD, 2001, p. 117).

At the operational and strategic levels, contingency planning appears to be used interchangeably with continuity planning, or minimally, contingency planning is devised for a specific situation when things could go wrong and is included as an element of continuity planning.

For example, in a DoD Inspector General (IG) Report on Contingency Planning for DoD Mission-Critical Information Systems, the report stated:

> The Federal Information Security Management Act requires that Federal agency information security programs provide, among other things, plans and procedures for the continuity of operations for agency information systems to continue operations during a disruptive or catastrophic event. This is called contingency planning. (DoD Inspector General, 2008, p. 5)

Furthermore, as it is relevant to the research topic, the results of the report speak to the lack of systems preparedness the DoD may face in the event of any system disruptions. Using the DoD Information Technology Portfolio Repository (DITPR) as the primary information source, the DoD IG reported that of 436 mission-critical information systems requiring information assurance certification and accreditation:

- 264 systems (61 percent) lacked a contingency plan or their owners could not provide evidence of a plan
- 358 systems (82 percent) had contingency plans that had not been tested or for which their owners could not provide evidence of testing
- 410 systems (94 percent) had incorrect testing information reported in DITPR
- 37 systems (8 percent) had incorrect contingency plan information in DITPR

As a result, DoD mission-critical systems may not be able to sustain warfighter operations during a disruptive or catastrophic event. Furthermore, the reported stated the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer did not implement management controls by establishing a comprehensive and overarching contingency planning policy (DoD Inspector General, 2008). Although the results of this audit cannot be extrapolated to other categories of systems, the results may provide an indication of the level of preparedness to continue or restore mission-critical systems in the event of a disruption.

Relevant Research Categories and Topics

Furthermore, as part of the literature review, key topics and subtopics were captured, and subsequently iteratively refined, for use in investigating continuity of operations related concepts in selected guidance documents (Appendix A). The topics were grouped into four overall categories. The subtopics were included to further clarify the topics; however, the list of subtopics was not meant to be all inclusive.

III. Research Methodology

"No-one is so brave that he is not disturbed by something unexpected."

- Julius Caesar

Introduction

This chapter presents the methodology employed to review United States Government and non-United States government guidance to discover existing risk management frameworks and identify common elements needed for continuity of operations planning. The chapter describes the design of the research study, details the research approach, discusses the content analysis methodology, explains the process for data collection and analysis, and lastly, discusses the limitations of the study.

Methodology and Research Strategy

Qualitative research is an "umbrella term" covering many different research strategies (Roberts, 2004, p.11). As such, determining the best research strategy to employ can be challenging; however, for this research a pure naturalistic-qualitative strategy was used from Patton's 2002 "Integrated Model of Measurement, Design, and Analysis" (Trochim & Donnelly, 2008). This strategy began with a naturalistic inquiry, in this case, "What written guidance is available identifying how to plan for and assure mission continuity after an incident?" A content analysis was then performed to investigate the inquiry.

Content analysis is a research tool used to determine the presence of certain words or concepts within texts, or sets of texts. Content analysis further provides a systematic and replicable technique for condensing the text into content categories (Berelson, 1952; Krippendorff, 2004). This type of analysis is used by the researcher to quantify and analyze the presence, meanings and relationships of such words and concepts, then make inferences about the messages within the texts, the writer, the audience, the culture, and time frame in that they were written. To conduct a content analysis on any such text, the text is coded, or broken down, into manageable categories on a variety of levels—word, word sense, phrase, sentence, or theme—and then examined using one of content analysis' basic methods: conceptual analysis or relational analysis (CSU, 2010).

Conceptual analysis establishes the existence and frequency of concepts, most often represented by words of phrases, in a text. In contrast, relational analysis goes one step further by examining the relationships among concepts in a text. Either of these analysis approaches can be applied to examine any piece of writing or occurrence of recorded communication and is used in marketing and media studies, to literature and rhetoric, ethnography and cultural studies, gender and age issues, sociology and political science, psychology and cognitive science, and many other fields of inquiry. In this study, a conceptual content analysis will primarily be used to "identify the intentions, focus or communication trends of an individual, group or institution" (Berelson, 1952).

The use of conceptual analysis requires the researcher first clearly develop their research questions and to select the documents to be analyzed. Next, the researcher must selectively reduce the texts to a set of categories consisting of a word, set of words or phrases. This enables the researcher to code specific words or patterns that are indicative of the research question. Once chosen, the texts must be coded into content categories. The process of coding is basically one of selective reduction (CSU, 2010).

Methodology Approach

Based on the selected conceptual content analysis methodology, an approach for the review of the United States government and non-United States government guidance needed to be designed.

United States Government Publications

There are thousands of DoD and Air Force policies. As of 26 March 2010, there were 1,352 DoD issuances, consisting of DoD Directives, Instructions, Publications, Directive-Type Memorandums, and Administrative Instructions listed on the DoD issuances web site (http://www.dtic.mil/whs/directives/). The issuances were categorized into eight major subject groups. As of 24 March 2010, there were 1,827 Air Force departmental publications categorized into 38 different publication series. The Air Force documents included in the publication series were Air Force departmental documents, such as Air Force Policy Directives (AFPD), Instructions (AFI), Manuals (AFMAN), and Pamphlets (AFPAM) hosted on the Air Force e-Publishing web site (http://www.e-publishing.af.mil/), the principal web source for accessing, viewing, and downloading electronic products.

To first narrow the body of information for the content analysis, the DoD issuance and Air Force departmental publication series were reviewed to determine what series of publications would be examined. To determine the DoD issuance series to investigate, the DoD Issuance Numbering System schema was reviewed. Based on the DoD major subject groups and subgroups numbering system for issuances (DoD, n.d.), two major subject groups were selected for investigation. The two subject groups were:

- Plans and Operations, Research and Development, Intelligence, and Computer Language (Series 3000 issuances)
- Information Management/Information Technology (Series 8000 issuances)

Within these two DoD major subject groups, four subgroups were selected for review; they were:

- Crisis Management and Emergency Preparedness (Series 3020 issuances)
- Mission and Functional Processes (Series 8200-8299 issuances)
- Vulnerability Management (Series 8531 issuances)
- Critical Infrastructure Protection (Series 8590 issuances)

To determine what series of Air Force publications to initially review, the publication series descriptions in AFI 33-360, *Publications and Forms Management*, 2006, were reviewed. Six Air Force publication series were selected for review (Appendix B).

Next, within each of series selected, each DoD issuance and departmental Air Force publication was briefly assessed to determine if the publication would be included in the content analysis sample. Specifically, the title and opening paragraph (purpose statement) of each publication was reviewed to decide if the publication addressed any of the research topics identified in Appendix A.

An a priori approach to coding was taken; as such, the topic categories were established prior to the analysis. As previously discussed, the list of topics and subtopics was constructed based on the key terms identified during periphery research and the literature review conducted in Chapter 2. Additionally, the topics were agreed upon between the researcher and a PhD professor closely familiar with the area of research, as well as reviewed by a handful of other professors and graduate students investigating other elements of this stream of research. Subtopics were added to further clarify the topics, and the subtopics were not meant to be all inclusive.

Each publication title and opening paragraph was subjectively reviewed for the following concepts and key words: mission, assurance, assessment, planning, continuity, crisis, emergency, disruption, disaster, impact, incident, threat, scenario, organizational resilience, infrastructure protection, vulnerability, and risk. Also, six document key-word searches were conducted during this cursory review; the key words were: continuity, incident, mission assurance, planning, recovery, and risk. The key terms were selected from the topics in Appendix A, and were the most relevant to the concepts being research in this content analysis.

Throughout these steps, the overall naturalistic inquiry statement (What written guidance is available identifying how to plan for and assure mission continuity after an incident?) remained in focus.

In addition to reviewing DoD and Air Force guidance, documents developed by the National Institute of Standards and Technology (NIST) were selected for content analysis. NIST, a non-regulatory agency of the United States Department of Commerce, has statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347 (E-Government Act of 2002), and is responsible for developing standards and guidelines for providing adequate information security for all agency operations and assets (NIST, 2004a).

NIST Special Publications in the 800 series were reviewed and publication selections were conducted using the same phased review approach detailed for DoD and Air Force publications.   The Special Publication 800 series reports on NIST Information Technology Library's (ITL) research, guidelines, and outreach efforts in computer security, and ITL's collaborative activities with industry, government, and academic organizations (NIST, 2010b).

Non-United States Government Publications

To complement and compare against the United States government publications, publications from four non-United States government bodies of knowledge were investigated for inclusion in the content analysis sample. First, international standards were considered. Since the International Organization for Standardization (ISO) is the world's largest developer and publisher of international standards (ISO, 2010), ISO publications were consider in the sample population. Specifically, publications from the ISO/ International Electrotechnical Commission (IEC) Information Security Management System (ISMS) family of standards (Series 27000) were reviewed for inclusion. Through the use of the ISMS standards, organizations can develop and implement a framework for managing security of their information assets and prepare for an independent assessment of their ISMS applied to the protection of information (ISO/IEC, 2009).

Second, IT Governance Institute's (ITGI) Control Objectives for Information and related Technology (COBIT$^{®}$) document was selected for inclusion. ITGI was selected because of their recognized effort to assist enterprise leaders in their responsibility to ensure IT is aligned with the business and delivers value, its performance is measured, its resources properly allocated, and its risks mitigated. ITGI exists to be the leading reference on IT governance for the global business community (ITGI, 2010).

Third, IT Infrastructure Library (ITIL) documents were considered for the content analysis. Developed in the late 1980's, the ITIL codifies industry best practices for the support and delivery of IT services and has become the world-wide de-facto standard in Service Management (Office of Government Commerce, 2000). The Air Force understands the Air Force-Global Information Grid requires an organized management methodology and recognizes ITIL as an IT management standard across both industry worldwide and DoD (Department of the Air Force, 2006c).

Lastly, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE^{SM}) criteria document was selected to be included as a publication sample. The OCTAVE work is conducted by Carnegie Mellon University and is sponsored by the DoD. OCTAVE enables organizations to understand and address their information security risks, and it is a comprehensive, systematic, context-driven, and self-directed evaluation approach (Alberts & Dorofee, 2001; Alberts, Dorofee, Stevens, & Wooky, 2003).

Instrumentation and Data Collection

After transitory reviews of the publications were completed using a naturalistic inquiry methodology and the sample documents were collected, the next step was to code the documents and collect qualitative data (Trochim & Donnelly, 2008). A Likert-like scale was developed to subjectively code the degree of concept coverage of each topic in a publication. The sample policies were assessed and coded for each of the 14 topics (Appendix B) using the content analysis coding scheme shown in Figure 3.

Coding Scheme	
1 =	No discussion of topic
2 =	Concept ***identified*** by name; but, not defined
3 =	Concept introduced by name; but, ***limited*** discussion (e.g., 1 of 3 noted: defined, examples, or strategies)
4 =	Concept introduced by name with ***moderate*** coverage of topic (e.g., 2 of 3 noted: defined, examples, or strategies)
5 =	Concept introduced by name with ***full*** coverage of topic (e.g., 3 of 3 noted: defined, examples, or strategies)

Figure 3. Content Analysis Coding Scheme

Multiple Coders

A content analysis method is a systematic process. Inferences from the analysis must be objective and the inferences by one researcher should be analogous to the inferences on another researcher with access to the same data. To make valid inferences, "it is important that the classification procedure be reliable in the sense of being consistent: Different people should code the same text in the same way" (Weber, 1990, p. 12).

One way to calculate reliability is to measure the percentage of agreement among coders (Stemler, 2001). However, this method does not take into account the fact that raters are expected to agree with each other a certain percentage of time simply by chance (Cohen, 1960). To account for chance, an inter-rater reliability analysis using the Cohen kappa coefficient statistical measure was also performed to determine consistency among raters. A kappa value of 0 implies no agreement, other than by chance. Conversely, a value of 1 corresponds to a perfect agreement between the two raters (Vanbelle & Albert, 2008). Krippendorff (2004) recommends a kappa agreement level of at least .70. Some scholars use a measure of .80 or greater (Denzin & Lincoln, 2000).

An on-line statistical computation tool developed by Dr. Lowry (2010), Vassar College, was used to calculate the kappa statistics. The weighted kappa was used because the coding data are ordinal (Lowry, 2010; Vanbelle & Albert, 2008) and the weighted kappa allows for “close” coding ratings not to simply be calculated as “misses” (TexaSoft, 2008). Table 2 shows the imputed relative distances between the ordinal categories used for the kappa statistics calculations.

Table 2. Kappa Weighting: Imputed Relative Distances

Successive Ordinal Categories	1~2	2~3	3~4	4~5
Imputed Relative Distances	1	1	1	1

For this content analysis, one researcher analyzed 100 percent of the sample publications and another researcher analyzed 50 percent of the publications. After scoring a few test publications together, the researchers worked independently on coding the sample publications. The publications examined by the second researcher were randomly chosen by selecting every other publication on the coding matrix. Also, while the second researcher was familiar with the overall CIMIA research project, the researcher was not unduly familiar with the topics investigated during the content analysis.

IV. Analysis and Results

"In the middle of difficulty lies opportunity."

- Albert Einstein

Introduction

This chapter presents the results and analysis of the research conducted. The publications selected for analysis are identified and the inter-rater reliability statistics are described. The data are analyzed with the intent of answering the research questions and are organized around the 14 topics analyzed during the content review. The findings include both qualitative and quantitative descriptions.

Publications Selected

Using the methodology detailed in Chapter 3, of 1,352 DoD issuances, 6 DoD issuances were selected for content analysis. Of the 1,827 Air Force departmental publications, 6 publication series were selected, 97 publications of interested were noted, and 36 publications were selected for content analysis (Table 3).

Table 3. Air Force Publications Reviewed

Air Force Pubs Series Number and Series Title	Number of Pubs in Series	Pubs Reviewed	Pubs of Interest	Pubs Coded
10 - Operations	148	148	51	21
31 - Security	54	54	6	1
32 - Civil Engineering	110	110	7	3
33 - Communications and Information	75	75	13	6
90 - Special Management	31	31	12	4
91 - Safety	68	68	8	1
Total	**486**	**486**	**97**	**36**

Air Force publications of interest were publications that did not met the naturalistic inquiry of this research and were not coded; however, the publications did have some relevance to the stream of research. As such, the researcher noted the publications and captured key text extracts from the publications. Text extracts were also collected for the Air Force publications selected for the content analysis sample. Appendices C through H provide the title, date, and text extracts for the publications of interest, as well as the publications selected for coding. As shown on the tables in the appendices, the publications chosen for the content analysis are highlighted to distinguish them from the publications of interest.

To complete the list of United States government publications included in the sample, nine NIST Special Publications in the 800 series (information technology security publications) were chosen for the content analysis.

Furthermore, nine publications from four non-United States government entities were selected for coding. As a result of the overall publications review, a total 61 documents were selected for content analysis.

Coding Results and Inter-rater Reliability

The coding results from the primary researcher are shown at Appendices I and J. The coding results of both researchers were analyzed and two measures of reliability were calculated: percentage of agreement among coders and Cohen's kappa. Two measures were calculated due to the strengths and weakness of each measure.

First, the percentages of agreement were computed and the statistics are shown in Table 4.

Table 4. Percentage of Agreement Between Coders

Topic	Percent Agreement	Number of Agreements	Number of Disagreements	Number of Disagreements Greater Than One Value
Mission Assurance	80.0%	24	6	0
Mission Assessment	86.7%	26	4	1
Mission to IT Dependencies	60.0%	18	12	2
Continuity Plan	43.3%	13	17	5
Preparedness	30.0%	9	21	1
Recovery	53.3%	16	14	1
Lessons Learned	63.3%	19	11	2
Scenario-Based Planning	66.7%	20	10	0
Organizational Resilience	66.7%	20	10	1
Critical Infrastructure Protection	70.0%	21	9	2
Risk Management	66.7%	20	10	1
Risk Assessment	50.0%	15	15	2
Incident Response	73.3%	22	8	0
Incident Notification	63.3%	19	11	1

Although the percentage of agreement for the topics varied from 30 to 86.7, the number of disagreements greater than one value on the coding scale was small. Of the 840 coding decisions made by the two coders, only 19 decisions (2.3 percent) were a result of disagreements greater than one value. For example, if one researcher coded a topic a “2” (concept identified) and the other researcher coded the same topic a “4” (concept moderately covered), the result would be a value difference of 2. Since the publications were coded on an ordinal scale (that is, a topic was coded from a minimum of not being discussed to a maximum of being fully discussed), these results suggest the researchers similarly coded the documents.

Next, the inter-rater reliability for the researchers for each of the 14 topics was calculated using Cohen’s kappa. The resulting kappa statistics and confidence intervals are show in Table 5.

Table 5. Kappa Statistic Results for Two Coders

Kappa with Linear Weighting					
Topic	Observed Kappa	Standard Error	.95 Confidence Interval		**Kappa Interpretation** (Landis & Koch, 1977)
			Lower Limit	Upper Limit	
Mission Assurance	0.5161	0.1509	0.2203	0.8119	Moderate
Mission Assessment	0.1964	0.2146	0.0000	0.6171	Slight
Mission to IT Dependencies	0.1463	0.0857	0.0000	0.3142	Slight
Continuity Plan	0.4241	0.1217	0.1856	0.6626	Moderate
Preparedness	0.4221	0.0815	0.2624	0.5818	Moderate
Recovery	0.6318	0.0803	0.4744	0.7892	Substantial
Lessons Learned	0.5752	0.1066	0.3663	0.7841	Moderate
Scenario-Based Planning	0.6795	0.0827	0.5174	0.8416	Substantial
Organizational Resilience	0.4444	0.1350	0.1798	0.7090	Moderate
Critical Infrastructure Protection	0.6577	0.0823	0.4964	0.8190	Substantial
Risk Management	0.7334	0.0738	0.5887	0.8781	Substantial
Risk Assessment	0.5438	0.1007	0.3464	0.7412	Moderate
Incident Response	0.7624	0.0793	0.6070	0.9178	Substantial
Incident Notification	0.5476	0.1214	0.3097	0.7855	Moderate

The observed kappa statistics ranged from 0.1463 to 0.7624. While unsupported empirically, the kappa interpretations are based on the suggested benchmarks identified by Landis and Koch (1977). The levels Landis and Koch proposed for interpreting kappa are listed in Table 6.

Table 6. Kappa Statistic Agreement Levels
(Landis & Koch, 1977, p.165)

Kappa Statistic	Strength of Agreement
<0.00	Poor
0.00- 0.20	Slight
0.21- 0.40	Fair
0.41- 0.60	Moderate
0.61- 0.80	Substantial
0.81- 1.00	Almost Perfect

All of the topics were coded with a kappa agreement level of either moderate or substantial, except for two topics. Mission assessment and mission to IT dependencies had a "slight" level of agreement. Although the kappa statistics were low for these two topics, the data suggest one reason may be the high level of agreement within just a few coding categories. For example, when the researchers coded the mission assessment topic, 25 samples (50 coding decisions) out of 30 samples fell within one coding category. This was the most samples coded in a single category of any topic. For the mission to IT dependencies topic, 26 samples were clustered within two coding categories. Strijbos, Martens, Prins and Jochems (2006) highlighted the concern of underestimating kappa agreement for a category that is commonly used, specifically as the number of categories available is increased.

Given the percentages of coding agreement, the ordinal nature of the coding scale, the subjectivity of the coding effort, the high percentage of exact and close proximity coding, the observed moderate to substantial kappa statistics, and most importantly, the intended use of the data, the data suggest the coding results are sufficiently reliable for this research effort.

Publication Authors

Of the 61 documents selected for analysis, the civil engineering community was the most prolific authors of government documents. The ISO authored the most non-government documents analyzed. Table 7 lists all of the organizations who published documents reviewed during the content analysis.

Table 7. Organizations Who Authored Publications Included in Content Analysis

Functional Community/Organization	No. of Pubs
HQ USAF: Civil Engineering (A7C)	13
National Institute of Standards and Technology; US Department of Commerce (NIST)	9
HQ USAF: Operations, Plans and Requirements (A3/5)	7
SECAF: Information Dominance and Chief Information Officer (A6)	6
International Org for Standardization/International Electrotechnical Commission (ISO/IEC)	6
Under Secretary of Defense for Policy (USD(P))	4
HQ USAF: Security Forces (A7S)	3
HQ USAF: Safety (SE)	3
IT Infrastructure Library - UK Office of Government Commerce (OGC)	2
HQ USAF: Plans and Requirements (A5)	1
HQ USAF: Analysis, Assessments and Lessons (A9)	1
Asst Secretary of Defense - Command, Control, Communications, and Intelligence (ASD(C3I))	1
Asst Secretary of Defense for Networks and Information Integration (ASD(NII)) / DoD Chief Information Officer (CIO)	1
Carnegie Mellon University (CMU)	1
HQ USAF: Inspector General (IG)	1
IT Governance Institute (ITGI)	1
HQ USAF: Surgeon General (SG)	1

Ranking of Topics

Based on the summation of the raw coding scores for each topic reviewed, the topics were ranked from the topics most discussed to the topics least discussed. For example, preparedness was found to be discussed the most within the government publications and as such, was ranked 1. Table 8 shows the rankings of all 14 topics with the results computed within each publication category (government or non-government).

Table 8. Topic Rankings (Most to Least Discussed)

US Governmental Publications		Non-US Governmental Publications	
Topic	**Ranking**	**Topic**	**Ranking**
Preparedness	1	Risk Assessment	1
Recovery	2	Preparedness	2
Risk Assessment	3	Risk Management	3
Risk Management	4	Continuity Plan	4
Lessons Learned	5	Incident Notification	5
Continuity Plan	6	Recovery	6
Incident Response	7	Lessons Learned	7
Scenario-Based Planning	8	Incident Response	8
Incident Notification	9	Scenario-Based Planning	9
Critical Infrastructure Protection	10	Mission to IT Dependencies	10
Mission Assurance	11	Critical Infrastructure Protection	11
Mission to IT Dependencies	12	Mission Assurance	12
Organizational Resilience	13	Mission Assessment	13
Mission Assessment	14	Organizational Resilience	14

Comparing the two rankings, topics typically ranked relatively close (plus or minus one ranking position) between the two publication categories (Table 9). The two exceptions were recovery and incident notification. Recovery ranked second in the government publications and sixth in topic coverage within the non-government publications. The inverse was true for incident notification. Incident notification ranked fifth in the non-government publications and ninth within the government publications.

Table 9. Topic Ranking Differences: Government vs. Non-Government Publications

Topic	Ranking Difference
Preparedness	1
Risk Management	1
Incident Response	1
Scenario-Based Planning	1
Critical Infrastructure Protection	1
Mission Assurance	1
Organizational Resilience	1
Mission Assessment	1
Risk Assessment	2
Lessons Learned	2
Continuity Plan	2
Mission to IT Dependencies	2
Recovery	4
Incident Notification	4

Top Reviewed Publications

Using the content analysis coding scale, each publication could receive a minimum score of 14 (lowest code of 1 multiplied by 14 topics) and a maximum score of 70 (highest code of 5 multiplied by 14 topics). Based on the summation of the raw coding scores for each publication reviewed, the top five publications with the greatest degree of topic coverage are listed in Table 10. No single publication fully covered each topic and received the maximum score of 70. COBIT v4.1 provided the most coverage of the 61 publications reviewed and, minimally, identified each of the concepts investigated.

Table 10. Ranking of Top Five Publications

Publication	Raw Score	Ranking
ITGI Control Objectives for Information and related Technology (COBIT) v4.1, 2007	48	1
NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems (Draft)* , 2009	43	2
ITIL Service Delivery v2, 2001	39	3
AFMAN 10-2504, *Air Force Incident Management Guidance for Major Accidents and Natural Disasters*, 2009	39	4
NIST Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, 2008	38	5

Results and Analysis of Topics

Mission Assurance

In a majority of the documents, mission assurance was not discussed and as such the topic was ranked in the lower tier for both government and non-government publications. However, mission assurance was defined in two publications. Both documents defined mission assurance as ensuring organizations can perform assigned tasks or duties in accordance with the intended purpose or plan (Department of the Air Force, 2006b; DoD, 2010). DoD’s framework for mission assurance includes a range of programs, e.g. risk management and security-related functions, with the intention of securing war fighting capabilities even when under attack or after disruption. These efforts include force protection measures, preparedness, continuity of operations plans, emergency management, consequence management, continuity of government, and critical defense infrastructure protection (Department of the Air Force, 2006b).

In light of these activities, successful missions do not just happen; they are indicators of how well a system is functioning. The contributors to successful missions are man, media, machine, and management. Mission then is the desired outcome, and the results of the interactions of the man, media, machine, and management (Department of the Air Force, 2000b).

Mission assurance was also discussed in the narrower context of information assurance and DoD information systems. DoD policies, implemented through AFI 33-200, *Information Assurance (IA) Management,* 2008, require DoD information systems to be assigned a mission assurance category (MAC) (DoD, 2002b, 2003). The categories are primarily used to determine the requirements for availability and integrity. Although the MAC's are directly associated with the importance of the information the systems contain relative to the achievement of DoD goals and objectives, the three-tier category classification system is system-centric.

Additionally, the IT Governance Institute advocates for the need for management to establish control objectives to reasonably assurance business (mission) objectives are achieved (COBIT v4.1, 2007). COBIT v4.1 defines control objectives for 34 processes (210 components); but, they are IT specific. However, the guidance does give a substantial framework for managing IT to assist with managing one element required in an overall effort to achieve mission assurance.

DoD Instruction 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*, 2008, also mentioned the concept of mission success and mandated a mission focus statement be produced specifying defense critical infrastructure performance standards and conditions necessary for mission success. However, the instruction does not specify examples or how to determine the necessary standards and conditions.

Although details beyond an overall framework and overarching concepts on how to assure the mission were not discovered, understanding the concept of mission assurance does appear to be important to the Air Force. One of the Counter-Chemical, Biological, Radiological and Nuclear (C-CBRN) Education, Training, and Exercise (ETE) competencies is to “understand mission assurance/continuation planning considerations and relationship to command, control, communications, computers and intelligence on Air Force installations” (Department of the Air Force, 2008d). C-CBRN ETE competencies are knowledge, skills, and abilities to be educated, trained, and exercised by the Air Force to realize its desired C-CBRN operational capabilities. These Air Force competency requirements are met collectively through various education and training program, including formal education and technical training; MAJCOM-level, base-level, other Service and other federal agency education and training; and appropriate civilian academic institutions. The competencies apply to all Air Force personnel, regardless of rank or Air Force specialty code (Department of the Air Force, 2008d).

Mission Assessment

Mission Assessment ranked as one of the least discussed topics in the sample. No formal definition of mission assessment, or the concept in general, was uncovered. However, there is a general sense of mission assessment or evaluation within the Inspector General (IG) system, considering IG teams focus on inspecting and grading mission performance.

Whether conducting an operational readiness inspection or compliance inspection, the IG assesses readiness, key processes, procedures, or requirements, based on by-law requirements, executive orders, and/or instructions. Among other items, but specific to this research, inspected units may be evaluated on whether the unit has a continuity of operations and if unit personnel know what actions to take during potential incidents. Unit's may also be assessed on their ability to conduct the full range of contingency operations while simultaneously responding to or recovering from incidents, such as natural disasters, attacks, etc. (Department of the Air Force, 2009c). The IG does provide a mission assessment snapshot in time; however, the IG process does not provide a standardized system of assessment or evaluation of the day-to-day missions conducted across the Air Force each day.

ITGI, in COBIT v4.1 (2007), noted the importance of measurable metrics to support business objectives. The measures are required for an organization to be graded a 4 (0 – 5 point scale) on their IT Processes, Organization, and Relationships Maturity Model. The document detailed potential metrics; however, the measures are IT focused.

Lastly, while overlapping risk assessment to an extent, one mission analysis tool of potential interest was noted – the mission protection tool. The mission protection tool focused on analyzing and protecting the mission, rather than on protection of personnel or things. The tool recognizes that a mission can be stopped partially or completely by events that cause very little damage. The mission protection analysis considers any source of mission interruption, not just those arising from traditional mishap sources. Two important resources for this analysis is a detailed mission statement and a diagram of key processes linked to the mission (Department of the Air Force, 2000b). While the mission protection analysis has no particular method, a potential example of the process used to select a set of tools for the mission analysis of a mission critical computer facility is described in Figure 4.

> **Situation:** A major material management center uses a computer to help manage the complex distribution and cost accounting needed to successfully carry out the mission. If this computer were to be seriously impaired in any way, the mission could be down for a time ranging from several hours to several days. The decision is made to complete an in-depth mission protection analysis of computer operation. The individual responsible for the applications uses his hazard ID toolbox to select the following tools for this important mission protection analysis.
>
> **TOOLS TO BE USED**
>
> Operations analysis (to establish the full dimension of the operation)
> What if analysis (to establish contingency-type threats to the mission)
> Interview tool (to get inputs from personnel involved in the operation)
> Several Logic Diagrams (used to explore several of the higher risk issues revealed by the tools above.)
> Interface tool (used to detect any threats from non-related functions)
> Change analysis tool (to assess any intentional or unintentional change in the last 1 or 2 years.)
>
> The products derived from this analysis is essentially the same as the hazard identification assessments except that the focus is on those things, whether they cause physical damage or injury or not, that impact the mission of the system.

Figure 4. Example Mission Protection Application (Department of the Air Force, 2000b, p. 60)

Generally, there appears to be a lack of Air Force mission metrics to evaluate mission performance.

Mission to Information Technology (IT) Dependencies

This topic was not frequently identified; however, the concept was veiled in a small number of government publications and more detailed in two NIST special publications and two non-governmental documents. A few government documents mentioned the need to identify and protect the vital records, databases, and software to execute mission essential functions and carry out continuity of operations plans (Department of the Air Force, 2005a, 2007, 2008e; DoD, 2006a, 2009a). However, guidance was limited to essentially identifying the concept.

NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, 2002, drew the linkage between IT systems and mission as well. In the publication, two interview questions are suggested to be asked to an organization during an IT system design phase. The questions are:

- What is the purpose of the system in relation to the mission?
- How important is the system to the user organization's mission?

Likewise, during the risk assessment process, NIST suggested collecting IT system mission (e.g., the processes performed by the IT system) and IT system and data criticality (e.g., the system's value or importance to an organization). However, value is aggregated to the system level, similar to system mission assurance codes, and does not address the potentially different values of data, information, and knowledge stored in one system.

NIST Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security,* 2008, provided guidelines on how to link the relationship between overall agency performance measures reporting and information security performance measures reporting to ensure an agency's information security program contributes to overall accomplishment of the agency mission, goals, and objectives. The security program measures are ultimately linked to IT resources.

COBIT v4.1 (2007) supported IT governance by providing an IT governance framework to ensure IT is aligned with the business. COBIT v4.1 provided a matrix of generic business goals and IT goals and shows how the generic examples can be used as a guide to determine the specific business requirements, goals, and metrics for an enterprise. COBIT v4.1 also illustrated how an enterprise strategy may be translated by the business into objectives related to IT-enabled initiatives (business goals for IT). These objectives may then lead to a clear definition of the IT goals. These IT goals in turn define the IT resources and capabilities (the enterprise architecture for IT) required to successfully execute IT's part of the enterprise's strategy.

Furthermore, ISO/IEC also suggested vital information required for the execution of an organization's mission be identified as part of information security risk management activities. Additionally, ISO discussed the importance of capturing the dependencies between business processes and assets (data, information, hardware) and provided examples of how dependencies may influence asset valuation (ISO/IEC, 2008).

Continuity Plan

In over half of the publications sampled, some type of continuity plan was at least identified. There were a few documents that covered the concept of a continuity plan to a greater extent.

DoDI 3020.42, *Defense Continuity Plan Development*, 2006, highlighted the criticality of determining accurate mission essential functions (MEF) to create the foundation of a valid continuity plan. The instruction further proposed two cyber-related mission essential areas of consideration: crisis communications and crisis data storage, retrieval, and security. The DoD guidance further detailed components of a continuity plan and what the plan's content should identify.

Comprehensive Emergency Management Plan (CEMP) 10-2 was noted as the primary installation plan to provide comprehensive guidance for emergency response to physical threats resulting from major accidents, natural disasters, conventional attacks, terrorist attacks, and chemical, biological, radiological and nuclear, and high-explosive (CBRNE) attacks. The CEMP is intended to be a separate installation plan and will not be combined with other plans until Headquarters Air Force develops and fields a template and provides implementation guidance. The plan addresses major accidents, natural disasters, enemy CBRNE attacks, and terrorist use of CBRNE (Department of the Air Force, 2007). However, the Emergency Management Program does not cover non-physical threats, including cyber threats. Associated non-physical hazards are the responsibility of the Air Force Deputy Chief of Staff, Air and Space Operations (Department of the Air Force Civil Engineer, 2006). While the intention is not to cover cyber threats in the CEMP, the research review suggests publications (e.g., AFI 10-211, *Civil Engineer Contingency Response Planning,* AFI 10-219V2, *Civil Engineer Disaster and Attack Preparations,* AFI 10-219V3, *Civil Engineer Disaster and Attack Recovery Procedures)* are focused on traditional infrastructure activities associated with planning, responding, and recovering from non-cyber threats. However, non-cyber hazards impact cyber resources that may ultimately impact mission continuation.

One AFI is dedicated to Air Force continuity of operations (COOP). The AFI discusses COOP policy and guidance, and COOP plan development. The instruction also provides guidance for developing programs to ensure continuity of essential operations of the Air Force across a wide range of potential emergencies. Furthermore, every organization is required to validate and update their COOP plan every 2 years (Department of the Air Force, 2005a).

ITIL's Service Delivery (2001) provided an example project plan for the efforts required to complete an IT service continuity plan. The project plan was broken down into four stages: initiation; requirements analysis and strategy definition; implementation; operational management.

NIST provided a table to collectively define the purpose of the various continuity plans as well as a plan's relationship to other plans or the organization. The types of plans identified in Table 11 are implemented individually or in coordination with one another, as appropriate, to respond to a disruptive event.

Table 11. Types of Plans (NIST, 2009, pp. 11-12)

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining business operations while recovering from a significant disruption.	Addresses business processes at a lower or expanded level from COOP mission-essential functions	Functional continuity plan that may be activated with a COOP to sustain non-critical functions.
Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's mission-essential functions at an alternate site for up to 30 days; mandated by federal directives.	Addresses the mission-essential functions; facility- based plan; information systems are addressed based only on their support to the mission-essential functions.	Functional continuity plan that may also activate several business unit- level BCPs.
Crisis Communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Pre-incident-based risk management plan that supports COOP plans for organizations with CI/KR assets.
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a system cyber attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	System contingency plan that may activate an ISCP or DRP, depending on the extent of the attack.
Disaster Recovery Plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	System contingency plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Location-independent plan that focuses on the procedures needed to recovery a system at the current or an alternate location.	System contingency-based plan that may be activated with a DRP or on its own if relocation is not required.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

Figure 5 shows the interrelationship of each plan as they are implemented to respond to the event as applicable to their respective scopes.

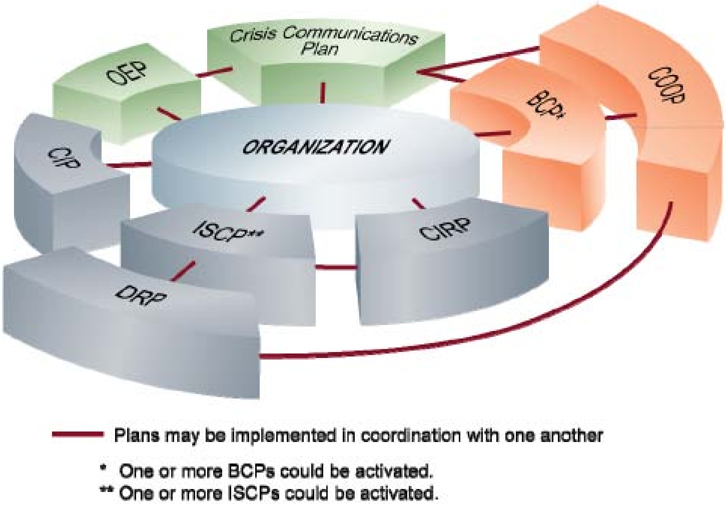
Crisis Communications Plan
OEP
CIP
ORGANIZATION
BCP*
COOP
ISCP**
CIRP
DRP
Plans may be implemented in coordination with one another
* One or more BCPs could be activated.
** One or more ISCPs could be activated.

Figure 5. Contingency-Related Plan Relationships (NIST, 2009, p. 12)

Lastly, there was a general lack of guidance regarding contingency plans in the communication and information series publication. Communications are sometimes considered in plans; but, typically from a long-established standpoint of command and control communications (e.g., telephones, radios, faxes, mass notification systems). The plans focused on communication-out procedures, such as using runners, flags, or flares, not on how information technology may be imbedded within critical processes and the true impact of disrupting communications.

Preparedness

Preparedness was one of the most discussed topics, and the concept, at the very least, was identified in 59 of the 61 publication analyzed. Preparedness was defined as:

> The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private-sector and nongovernmental

> organizations to identify threats, determine vulnerabilities, and identify required resources. (Department of the Air Force, 2009a, p. 71)

To be prepared, organizations should engage in contingency planning. Now that business processes are typically heavily dependent on IT, continuity planning incorporates a business element and a technology element (Office of Government Commerce, 2001).

To ensure business continuity and neutralize interruptions from information systems failures or disasters, in an effort to protect critical business activities and processes, ISO/IEC described five activities and controls organizations should implement. The activities included: including information security in the business continuity management process, performing continuity and risk assessments, developing and implementing continuity plans, maintaining a business continuity planning framework, and testing, maintaining and reassessing business continuity plans (ISO/IEC, 2005). IGTI details the same, and a few additional, activities and controls in COBIT v4.1 (2007); but, the COBIT-recommended actions are more heavily focused on IT continuity planning.

ITIL's Service Delivery (2001) provided comprehensive guidance on IT service continuity management. The document discussed the goal, benefits, scope, and concepts of IT continuity. Also, the document provided key messages, hints, tips, examples, and strategies on planning, implementing, and operationalizing IT continuity.

Finally, the Defense Continuity Program noted making the appropriate use of IT solutions "within the continuity operating environment to provide information to leaders and other users, facilitate decision making, and issue orders and direction" (DoD, 2006a,

p. 2). Also, as previously mentioned one AFI is dedicated to Air Force continuity of operations and provides guidance for developing programs to ensure continuity of essential operations of the Air Force (Department of the Air Force, 2005a). However, research suggests there is little provided DoD guidance specific to IT service continuity management.

Recovery

Overall, this topic was identified in about 80 percent of the publications reviewed. Recovery was the second most discussed topic in the sampled government publications, and sixth in topic coverage within the non-government publications.

Recovery was defined as:

> The development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private-sector, nongovernmental, and public assistance programs that: identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents. (Department of the Air Force, 2007, p. 123)

The DoD specifically included cyber resource restoration in their definition of cyber security. Cyber security “also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster” (DoD, 2010).

A majority of the Air Force publications that discussed recovery to any depth were discovered in the 10-series (civil engineering) publications. These civil engineering publications were principally dedicated to the recovery of facilities, infrastructure (roads, runways), and utilities. Additionally, the Air Force civil engineering community dedicated an entire 188-page publication to disaster and attack recovery procedures (Department of the Air Force, 2008c). Communications were mentioned; however, predominately from a command and control perspective.

NIST provided recovery guidance specific to IT systems. NIST defined recovery phase efforts as those activities focusing on recovery strategies executed to restore system capabilities, repair damage, and resume operational capabilities. Also, they provided information on the sequence of recovery activities, recovery procedures, and escalation and notification procedures (NIST, 2009).

Furthermore, ITIL suggested using a Component Failure Impact Analysis (CFIA) to provide estimated recovery times to help provide timely and accurate estimations of IT service restoration in an effort to manage the impact of IT failures. CFIA was devised by IBM in the early 1970's and can provide valuable information, such as single points of failure, impacts of component failure, component dependencies, and recovery timings, if the analysis is performed thoroughly. The CFIA is performed by mapping configurations items (e.g., computers, applications, power, etc) to IT services having a dependency on the configuration item. Another mapping is also completed, connecting the configuration items to vital business functions and the end users impacted by the configuration item. Ultimately, the mappings help estimate recovery times, provide alternate recovery options, and highlight dependencies (Office of Government Commerce, 2001). However, the scalability of this approach may be questionable.

Lessons Learned

This topic was moderately covered in the guidance analyzed. However, most of the substantial guidance was provided in government publications. The principle Air Force publication focused on lessons learned is AFI 90-1601, *Air Force Lessons Learned Program*, 2008. In the AFI, a “lesson learned” is defined as “an insight gained that improves military operations or activities at the strategic, operational, or tactical level, and results in long-term, internalized change to an individual, group of individuals, or an organization” (2008a, p.3). The purpose of the program is to enhance readiness and improve combat capability. Lessons may be applicable to training, exercises, experiments, and real-world events and the AFI provided an observation/lesson learned template for capturing lessons learned as well as prescribed after-action report forms.

To document and track lessons learned the Air Force uses the Joint Lesson-Learned Information System (JLLIS). Anyone may make a lesson learned submission using the web-based JLLIS (unclassified: https://www.jllis.mil/USAF; classified: http://www.jllis.smil.mil/USAF). Access to JLLIS capabilities and lessons learned data is tiered to ensure sensitive information is protected (Department of the Air Force, 2009b). Validated lessons learned may be “pushed” when a lessons-learned specialist identifies the target audience to push the information to or “pulled” by ad hoc queries. Figure 6 shows the relationships of the different elements of the process.

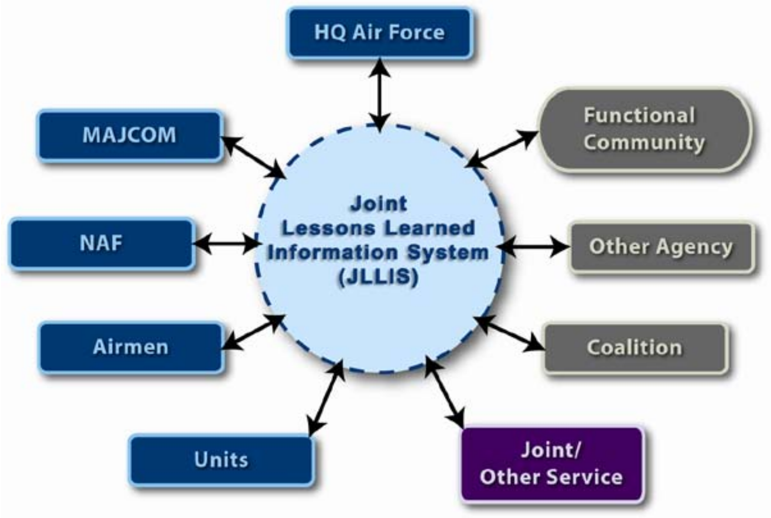

Figure 6. Air Force Lessons Learned Process (Department of the Air Force, 2009b, p. 30)

The civil engineering community codified some of their historical energy disruptions experience gathered as a result of inspector general tests, unplanned outages, and personal experiences. A list of 67 observed or projected disruption effects were published (Department of the Air Force, 2008b). By documenting and cross feeding lessons learned, resource protection is greatly enhanced (Department of the Air Force, 2009b).

Regardless of how the lessons-learned observations are collected, to ensure validated Air Force and Joint lessons are incorporated into programmatic and risk assessment decision cycles, the Headquarters Air Force Office of Lessons Learned is charged with coordinating with other Headquarters Air Force directorates on this task. Also, to facilitate use of lessons learned, lessons learned staff, at all levels, should participate in staff meetings, manning the Crisis Action Team, and/or providing real-time inputs to the commander’s planning and decision process (Department of the Air Force, 2008a).

Additionally, NIST noted one of the most important aspects of incident response is also the most often omitted—learning and improving. NIST proposed holding a lessons-learned meeting after significant incidents, and periodically after minor incidents, to improve security measures and the incident handling process. Furthermore, collecting lessons learned data may be used to justify additional funding for incident responses, measure the success/activities of the incident response team, and capture required data for any incident response reporting requirements (NIST, 2008a). Similarly, ISO recommended that to learn from information security incidents, mechanisms should be implemented to monitor and quantify the types, volumes, and cost of information security incidents (ISO/IEC, 2005, 2009).

Scenario-Based Planning

Scenario-based planning was also moderately covered in the guidance analyzed. The guidance did not cover the topic in depth; however, two tools were discovered to aid in creating scenarios—the scenario process tool (also known as the mental movie tool) and the “what if” tool. The scenario process tool is a procedure used to identify hazards by visualizing them. The process adds rigor to the intuitive and experimental process of traditional risk management, connects various individual hazards into scenarios, and assists in visualizing the worst credible outcomes of related hazards. Also, the “what if” tool is a practical and effective tool for identifying hazards; the tool is particularly effective in capturing hazard data about failure modes (Department of the Air Force, 2000b).

Specific to IT scenario-based planning NIST noted, “Scenarios provide an inexpensive and effective way to build incident response skills and identify potential issues with incident response processes” (NIST, 2008a, p. B-1). They proposed 20 scenario questions in the areas of preparation; detection, analysis, containment, eradication, recovery, and post-incident activities, along with 16 scenarios, that organizations may adapt for use in their own incident-scenario exercises. Additionally, ISO provided a list of examples of vulnerabilities and threats to help develop relevant incident scenarios. Furthermore, ISO suggested mapping the consideration of the likelihood of an incident scenario against the estimated business impact, in an effort to evaluate the measured risk against risk acceptance criteria (ISO/IEC, 2008).

Organizational Resilience

Organizational resilience was one of the least discussed topics in the publications reviewed. However, NIST did summarize organizational resiliency by stating, “Resiliency is not a process, but rather an end-state for organizations” (NIST, 2009, p. 5). Resilient organizations ensure continuity of operations during any type of disruption and they work to adapt to changes and risks that may impact their ability to continue critical functions. An organization’s resiliency program should include such activities as risk management, contingency, and continuity planning (NIST, 2009).

Organizations also have a style or a culture and this organizational culture may affect risk controls (actions designed to reduce risk). AFPAM 90-902, *Operational Risk*

Management (ORM) Guidelines and Tools, 2000, discussed the importance of developing risk controls consistent with an organization's culture. For example, a rigid, centrally directed risk control would be incompatible with an organizational culture that emphasizes decentralized flexibility.

Critical Infrastructure Protection

This topic was marginally identified in the documents analyzed. Notwithstanding, the DoD has two principle documents focused on critical infrastructure protection: DoDD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, 2010, DoDI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*, 2008. The DoD recognized the need to associate critical infrastructure with cyber resources, and the DoD Chief Information Officer is tasked with coordinating with the Under Secretary of Defense for Policy on integrating defense industrial base cyber security and information assurance activities in the DCIP (DoD, 2010).

The leading Air Force publication in this area was AFPD 10-24, *Air Force Critical Infrastructure Program (CIP)*, 2006. The DoD publications did not explicitly define critical infrastructures; however, AFPD 10-24 (2006) defined critical infrastructure as "cyber and physical systems and assets so vital to the Air Force that the incapacity or destruction of such systems and assets would have a debilitating impact on the Air Force's ability to execute its missions" (p. 10). In the Air Force definition, cyber systems are clearly included. For the Air Force Critical Infrastructure Program, criticality is broken down into four tiers (Department of the Air Force, 2006a):

- Tier I: Warfighter/Combatant Commands suffers *strategic mission failure*.
- Tier II: The Air Force *suffers mission failure*, but warfighter strategic mission is accomplished.
- Tier III: *Individual element failures,* but no debilitating strategic or Air Force mission failure.
- Tier IV: Everything else.

Risk Management

Risk management was a topic included in a majority of the publications reviewed, ranking as the fourth most discussed topic among government publications and the third most covered topic within non-government publications. Twelve definitions of risk management were noted during the review. The definitions were consistent with the description of risk management in JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 2001. Risk management is defined in JP 1-02 as the "process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits" (2001, p. 470).

As previously discussed, cyber systems are classified as part of the defense critical infrastructure (DCI) (Department of the Air Force, 2006a, DoD, 2010). This linkage is important as risk management principles are mandated for the DoD DCI Program (DCIP), and thus, for the inclusive cyber infrastructure and dependencies. The DoD policy expressly directed:

- Coordination on risk management shall be accomplished with other Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries, as appropriate
- DCI risk management actions shall:
  - Be coordinated and accomplished by responsible authorities
  - Support incident management
  - Protect DCI-related sensitive information
- DCIP shall coequally complement and not be subordinate to other DoD programs, functions, and activities that contribute to mission assurance through risk management
- The DCIP shall:
  - Determine the risks to DCI
  - Implement DoD-wide procedures to respond to risks to DCI and work with other Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries, as appropriate
  - Support and advocate for initiatives to respond to risks to national critical infrastructure as appropriate and within DoD legal authorities
  - DCIP activities related to the defense industrial base shall be consistent with and executed pursuant to the authorities established in the policy (DoD, 2010)

Of note in the policy are the strong support of risk management, the support of incident management, and the idea of associating risk management as a contributing activity to mission assurance. Essentially, the DCIP is a risk management program to ensure DCI availability. Figure 7 illustrates the DCIP Risk Management Process Model.

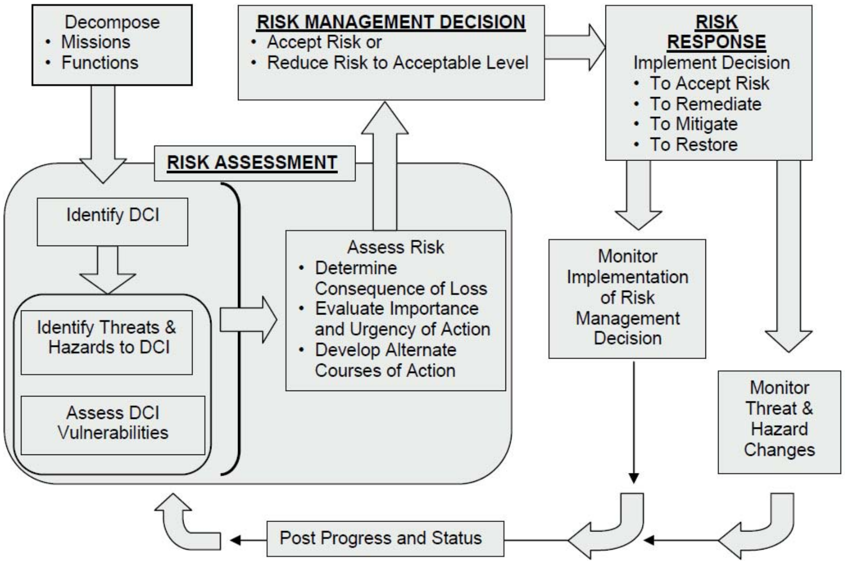
Decompose
• Missions
• Functions
RISK MANAGEMENT DECISION
• Accept Risk or
• Reduce Risk to Acceptable Level
RISK RESPONSE
Implement Decision
• To Accept Risk
• To Remediate
• To Mitigate
• To Restore
RISK ASSESSMENT
Identify DCI
Identify Threats & Hazards to DCI
Assess DCI Vulnerabilities
Assess Risk
• Determine Consequence of Loss
• Evaluate Importance and Urgency of Action
• Develop Alternate Courses of Action
Monitor Implementation of Risk Management Decision
Monitor Threat & Hazard Changes
Post Progress and Status

Figure 7. DCIP Risk Management Process Model (DoD, 2008, p. 16)

Important to note, the DCIP process model requires continuous coordination between mission and asset owners (DoD, 2008).

The Air Force formalized risk management through the concept of Operational Risk Management (ORM). ORM is defined as “the systematic process of identifying hazards, assessing risk, analyzing risk control options and measures, making control decisions, implementing control decisions, accepting residual risks, and supervising/reviewing the activity for effectiveness” (Department of the Air Force, 2000a). The ORM definition maps to the Air Force six-step ORM process (Figure 8).

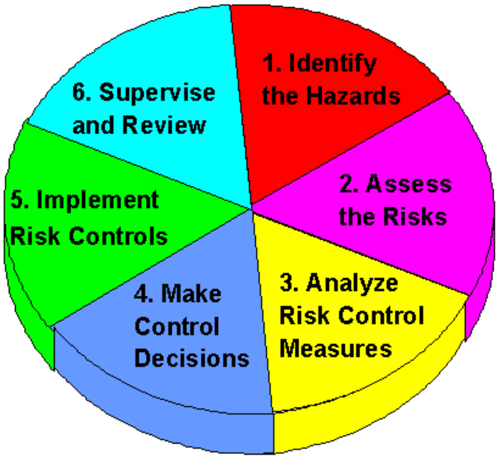
1. Identify the Hazards
2. Assess the Risks
3. Analyze Risk Control Measures
4. Make Control Decisions
5. Implement Risk Controls
6. Supervise and Review

Figure 8. Six-Step Process of Operational Risk Management (Department of the Air Force, 2000b, p. 7)

The Air Force discussed the importance of integrating the ORM process with mission processes, and having commanders dedicate the time and resources to incorporate risk management principles specifically into the planning processes. Integrating risk management into planning provides decision makers the greatest opportunity to control risk (Department of the Air Force, 2000a, 2000b). Also, during recovery operations, the installation commander will use operational risk management tools to decide the critical missions to continue (Department of the Air Force, 2009a).

While the Air Force ORM process may be applied across mission areas, NIST developed a six-step process risk framework specific to information systems (Figure 9).

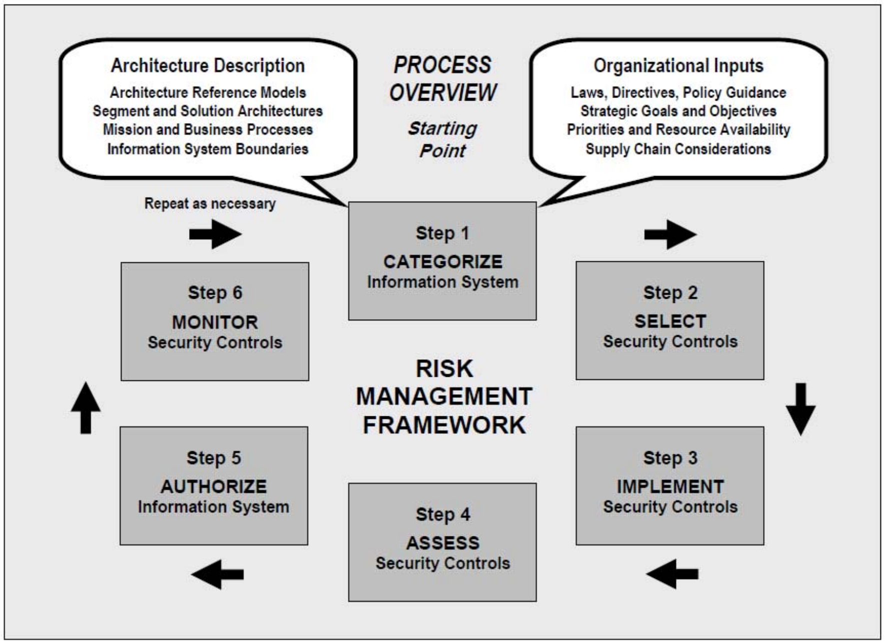
Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Figure 9. NIST Risk Management Framework (NIST, 2010a, p.8)

NIST also recognized the need for a consistent and effective approach to risk management, coupled with the necessary resource allocation (funding and personnel), in order for risk management to succeed (NIST, 2010a).

The non-government publications focused primarily on information systems/security risk management. However, the guidance also recognized risk management as a continuous process. ISO’s information security risk management process consists of six elements: context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review (see Figure 10) (ISO/IEC, 2008).

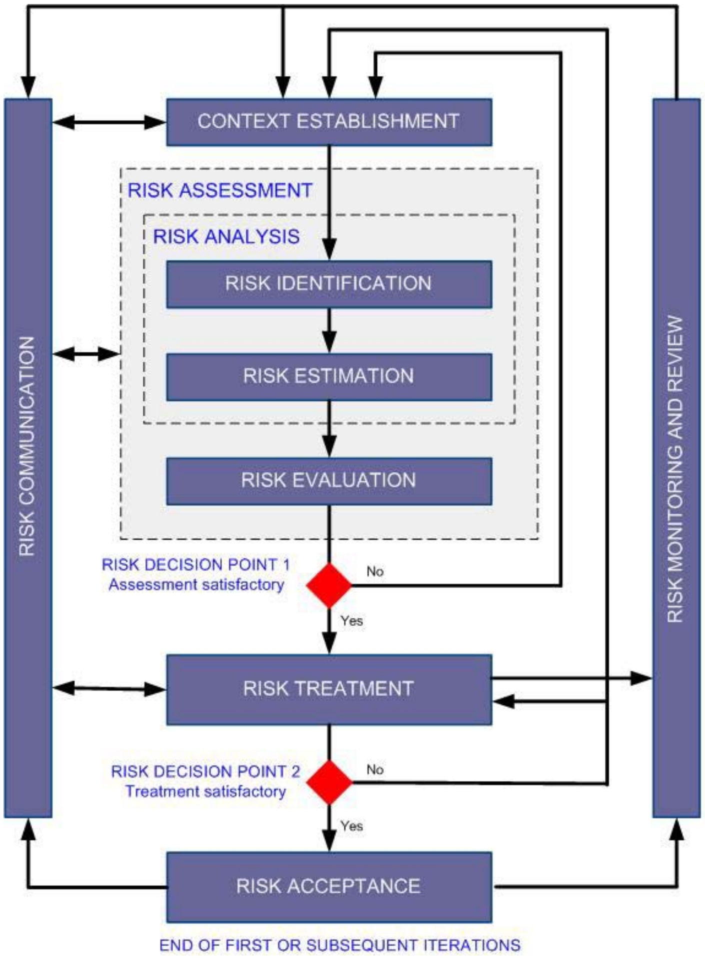

Figure 10. Information Security Risk Management Process (ISO/IEC, 2008, p. 5)

COBIT v4.1 identified five IT governance focus areas; these are areas executive management should address to govern IT across their enterprises. Risk management was one of the five focus areas, and the other four are: strategic alignment, value delivery, resource management, and performance measurement. The risk management area requires such focus as, risk awareness by senior leaders, an understanding of the enterprise’s appetite for risk, and embedding risk management responsibilities into the organization. The COBIT v4.1 document also noted the importance of identifying, analyzing, and assessing any potential impact of the goals of an organization as the result of any unplanned event. Furthermore, the following IT risk management related metrics were suggested in COBIT v4.1 (2007, p. 65):

- Percent of IT budget spent on risk management (assessment and mitigation) activities
- Frequency of review of the IT risk management process
- Percent of approved risk assessments
- Number of actioned risk monitoring reports within the agreed-upon frequency
- Percent of identified IT events used in risk assessments
- Percent of risk management action plans approved for implementation

Again, with a focus on information security risks, OCTAVE Criteria v2 (2001), detailed three risk management principles common to effective risk management approaches. The three broad principles are: Forward-Looking View, Focus on the Critical Few, and Integrated Management. The "Forward-Looking View" requires organization's to think about tomorrow's risks and focusing on managing the uncertainty. The "Focus on the Critical Few" requires organization's to focus on the most critical information security issues. The "Integrated Management" principle requires integrating information security issues with business processes and considering business strategies and goals when developing security strategies.

Lastly, a few Air Force documents referred to Air Force Tactics, Techniques, and Procedures 3-2.34, *Multi-service Tactics, Techniques, and Procedures for Risk Management*; but, the publication was rescinded on 19 August 2008 (Air Force e-Publishing, n.d.).

Risk Assessment

Risk assessment was one of the most discussed of the 14 topics, ranking as the third most discussed topic among government publications and the number one covered topic within non-government publications. Sixteen definitions of risk assessment were noted during the review, and the definitions focused on detecting hazards and threat, criticality, and vulnerability assessments. Generally, the definitions discovered were consistent with the description of risk assessment in Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 2001. Risk assessment is defined in JP 1-02 (2001, p. 470) as "the identification and assessment of hazards (first two steps of risk management process)." The Joint risk management process included three processes—identifying, assessing, and controlling risks (DoD, 2001).

DoDD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, 2010, expanded on the Joint publication definition of risk assessment and further described risk assessment as "a systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks" (p. 20). However, risk assessment (i.e., criticality determination, threats and hazards assessment, and vulnerability assessment), along with risk response (i.e., remediation, mitigation, and reconstitution), were clearly noted as the major elements of DCIP risk management (reference Figure 7). Additionally, the requirement to coordinate the recommendations, support information, decisions, etc., between DCI owners and mission owners was noted again (DoD, 2008).

Since risk assessment is encapsulated within the risk management process, the methods of evaluating and assessing risks are captured within most of the risk management frameworks presented in the previous risk management section. In addition to the other processes presented, NIST (2002) advocated for an IT system risk assessment methodology encompassing nine primary steps; the main steps are:

- Step 1 - System Characterization
- Step 2 - Threat Identification
- Step 3 - Vulnerability Identification
- Step 4 - Control Analysis
- Step 5 - Likelihood Determination
- Step 6 - Impact Analysis
- Step 7 - Risk Determination
- Step 8- Control Recommendations
- Step 9 - Results Documentation

Specific to information security risk management, risk assessment determines the value of the information assets, in addition to identifying applicable threats and vulnerabilities, identifying existing controls, determining the potential consequences, prioritizing the derived risks and ranks them against the risk evaluation criteria. Furthermore, to bound and scope a risk assessment, assets need to be identified (hardware, software, etc) (ISO/IEC, 2008).

ITIL's Service Delivery provided a list of risks and threats to be considered by IT managers. Alternatively, ITIL mentioned some risks that are "out of scope" of IT risk assessments; for example, changes in business direction, diversification, and restructuring (Office of Government Commerce, 2001, p. 170).

Lastly, while likely never applied to a "cyber mishap" yet, AFI 91-204, *Safety Investigation and Reports,* 2008, recognized "Risk Assessment – During Operations" as a possible judgment and decision-making error categorized in the Department of Defense Human Factors Analysis and Classification System, as a means for studying mishap incidents. A “Risk Assessment – During Operation” is described as a “factor when the individual fails to adequately evaluate the risks associated with a particular course of action and this faulty evaluation leads to inappropriate decision and subsequent unsafe situation. This failure occurs in real-time when formal risk-assessment procedures are not possible” (Department of the Air Force, 2008f, p. 117). There is also a category code for violations based on risk assessment. A “Violation – Based on Risk Assessment” is a “factor when the consequences/risk of violating published procedures was recognized, consciously assessed and honestly determined by the individual, crew or team to be the best course of action. Routine "work-arounds" and unofficial procedures that are accepted by the community as necessary for operations are also captured under this code” (Department of the Air Force, 2008f, p. 118).

Incident Response

Incident response was moderately discussed among both categories of publications, ranking in the middle tier of the 14 topics assessed. Over half of the publications did not identify the concept. The civil engineering community provided detailed response guidance in AFMAN 10-2502, *Air Force Incident Management System (AFIMS) Standards and Procedures*, 2009, and AFMAN 10-2504, *Air Force Incident Management Guidance for Major Accidents and Natural Disasters*, 2009; however, as noted previously, the procedures are focused on facilities, infrastructure (roads, runways), and utilities. However, the Air Force Incident Management System (AFIMS) discussed within the publications was prominent.

AFIMS was developed to ensure military service compliance and consistency with Presidential and DoD directives for all-hazards emergency prevention, preparedness, response, recovery, and mitigation operations. The system is used to organize and direct emergency response forces during incident management activities (Department of the Air Force, 2009b). No explicit mention of cyber-related incidents or responses was discovered in the publication. Also, no reference of AFMAN 10-2502 or AFIMS was found in the principle network operations incident notification publication, AFI 33-138, *Enterprise Network Operations Notification and Tracking*, 2005. However, AFIMS is stated to support Homeland Security Presidential Directive 5, *Management of Domestic Incidents*, and the National Response Framework (Department of the Air Force, 2009b). Within the National Response Framework (guide to how the Nation conducts all-hazards response), cyber incidents are one of the seven broad incident categories noted (Department of Homeland Security, 2008).

Regarding IT specifically, NIST Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, 2008, provided very detail guidance on cyber-related incident response. The publication outlined possible incident response team structures, detailed the basic incident handling steps and provides advice for performing incident handling more effectively, and provided specific recommendations for handling five types of incidents (denial of service, malicious code, unauthorized access, inappropriate usage, and multiple component).

Furthermore, NIST proposed a four-step incident response life cycle (Figure 11). The process is a continuous cycle, and as an outcome of post-incident activities, “lessons learned” are analyzed and may be used in the preparation phase.

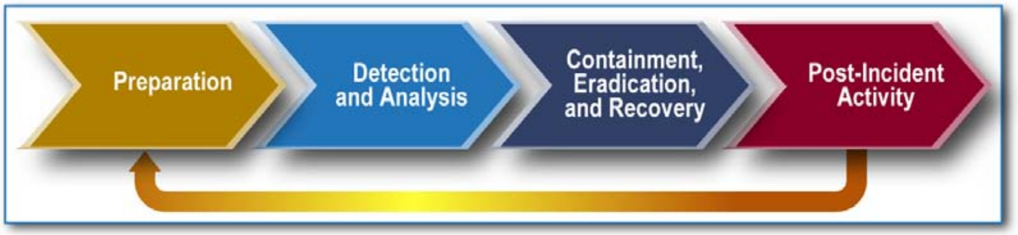

Figure 11. Incident Response Life Cycle (NIST, 2008c, p. 3-1)

Incident Notification

Incident notification ranked ninth within the government publications and fifth in the non-government publications. An incident (outage or disruption) may occur with or without prior notice and as such, notification procedures should cover both situations.

Prompt notifications are important for reducing the effects of a disruption on systems. However, activation criteria for system outages or disruptions are unique for each organization and should be stated the organization’s policy. Criteria may be based on the extent of any damage to the system (e.g., physical, operational, or cost); criticality of the system to the unit’s mission; and expected duration of the outage lasting longer than previously stated or expected (NIST, 2009).

AFI 33-138, *Enterprise Network Operations Notification and Tracking*, 2005, is the primary Air Force guidance for IT related incident notifications. The AFI provided guidance and explained the processes used by Air Force Network Operations to generate, disseminate, acknowledge, implement, track, and report network compliance and status information. AFI 33-138 dictated the use of Command, Control, Communications, and Computers Notice to Airmen (C4 NOTAM) as the primary means for notifying organizations of an information incident that may impact their operations. Within each organization, there is an individual who is responsible for reading incoming C4 NOTAMs and, when appropriate, is responsible for alerting decision makers within the organization about the significance of the C4 NOTAM with respect to the organizational mission. In certain cases where the network operations personnel understand the percieved criticality of an impacted resource, organizations are required to acknowledge receipt of the C4 NOTAM for accountability purposes.

Lastly, in addition to internal notification of incident, an organization may need to communicate with external partners regarding an incident. While minimum coordination may be specified for an organization by law or other directives, NIST also recommended considering coordinating with the outside parties show in Figure 12.

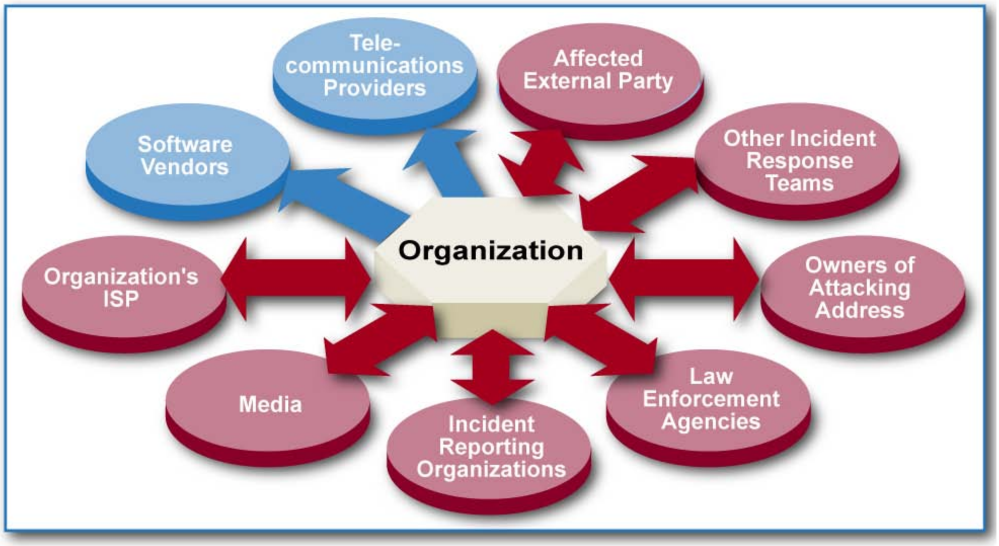
Tele-communications Providers
Affected External Party
Software Vendors
Other Incident Response Teams
Organization
Organization's ISP
Owners of Attacking Address
Media
Law Enforcement Agencies
Incident Reporting Organizations

Figure 12. Incident-Related Communications with Outside Parties (NIST, 2008c, p. 2-5)

Summary

Overall, the level of coverage of the 14 topics in the government and non-government publications closely mirrored one another. No single document provided full coverage of every topic; however, ITGI's *Control Objectives for Information and related Technology (COBIT)* v4.1 (2007) received the greatest number of coding points (48 out of maximum of 70), and, minimally, each of the topics was identified in the document. AFI 33-101, *Commanders Guidance and Responsibilities*, 2008, was coded the lowest, garnering a score of 16 (minimum possible score was 14).

Additionally, with an overall interest in the cyber-related aspects of mission assurance, generally the data suggest a low level of guidance being authored by the communications and information community regarding these 14 topics. Of the publications reviewed in the Air Force Communications and Information 33-series, only 5 of the 70 coding decisions resulted in a score above "3." Two of the five higher scores were attributed to one publication, AFI 33-138, *Enterprise Network Operations Notification and Tracking*, 2005.

V. Discussion and Conclusions

"We can't solve problems by using the same kind of thinking we used when we created them."

- Albert Einstein

Introduction

This chapter presents conclusions based on the content analysis conducted during the study. The six research questions identified in Chapter 1 are also summarily re-examined and conclusions are presented. Limitations of the research are also explained, and recommendations are provided. Then, the chapter concludes with areas for future research.

Research Summary

Overall, the amount of government guidance addressing the 14 topics in this study exceeded the researcher's expectations, especially within the NIST series of publications. The civil engineering community authored a large number of the government publications reviewed. The civil engineering community provided solid guidance on several of the traditional preparedness topics; however, some of their guidance may need to be expanded to include cyberspace resource preparedness issues or, at least, provide linkage to cyberspace preparedness guidance, largely yet to be developed, within the communications and information community.

Although the DoD is a large, highly complex organization that is not easily compared to other executive departments or private enterprises (Donley, 1995), the non-

United States government publications provided insights and significant coverage of some of the topics investigated. However, given the considerable size, complexity, and decentralized nature of the DoD and the fact non-government publications focus on organizations far smaller than DoD, the scalability of some of non-government solutions and recommendations may need to be fully evaluated.

Research Questions Reexamined

Research Question 1.

What is mission? Mission was seldom defined explicitly within the publications or issuances. However, based on the literature reviewed, a mission is essentially a task linked to a purpose. Mission requirements are communicated through mission essential task lists (METL). METLs are hierarchal and originate at the Joint Chiefs of Staff level and extend down to the operational level. However, there is an effort underway to extend METLs down to the unit level.

Extending METLs to the unit level should assist with identifying IT to mission dependencies, as the unit-level IT dependencies could be linked to unit- level tasks and activities. Furthermore, if these linkages can be integrated with the proposed Defense Readiness Reporting System (Secretary of Defense, 2006), this consolidated view would further enhance the situational awareness of commanders and decision makers as it would include related cyber dependencies specific to their organization's mission and tasks.

Research Question 2.

What is mission assurance? Mission assurance was also an elusive term in the publications reviewed; however, mission assurance was recently defined in DoD Directive 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, 2010. DoD defined mission assurance as a process to ensure tasks or duties can be performed in accordance with the intended purpose or plan. Furthermore, mission assurance is a summation of the activities and measures taken to ensure required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy. What appeared to be largely absent in the guidance was what control objectives or critical success factors (or the like) could be measured, so as to have observable, measurable mission success metrics.

As with mission, the foundational element appeared to be a task. As such, if a task is successful/may be assured, multiple successful tasks may be aggregated to assure objectives and missions. However, a challenge may arise when only some of the tasks are successful; then it becomes questionable if an aggregated mission is successful or assured. This challenge further supports the need for some form of mission measurements/metrics.

Research Question 3.

What are risk management and risk assessment, and how are they used to support mission assurance? Risk management was frequently defined in policy. Risk management is an overall process or program, and the process essentially involves identifying, assessing, and controlling risks, and furthermore, making decisions balancing risk costs with mission benefits. The Air Force specifically designed a six-step operational risk management process consisting of: identifying hazards, assessing risk, analyzing risk control options and measures, making control decisions, implementing risk controls, and supervising/reviewing the activity.

Risk assessment is a subset of risk management, and fundamentally involves the first two steps of risk management—identifying and assessing risk. Risk assessment provides an environment for decision makers to evaluate and prioritize risks and to recommend strategies to eliminate or mitigate those risks.

Also, risk management and assessment activities should be built into operational process. The activities should not be added on top of existing process, but rather, integrated within the processes to help ensure the risk management principles are used and the benefits garnered.

Furthermore, risk management and assessment facilitate mission assurance by remediating or mitigating risk and hopefully, as such, these activities reduce the probability of mission failure. In the context of infrastructure risk, the Defense Critical Infrastructure (DCI) Program supports a risk management process seeking to ensure DCI availability. The DCI Program risk management process is comprised of a risk assessment component that identifies critical assets and infrastructure interdependencies supporting DoD missions. Ensuring critical infrastructure availability in turn supports the tasks that make up a mission, thus, ultimately aiding in assuring the mission. However, in the cyberspace domain, risk needs to be managed and assessed beyond availability. There are other considerations, such as the confidentiality and integrity of information resources, that must be evaluated.

Research Question 4.

How are risk management and risk assessment conducted in military and non-military environments? As the content analysis illustrated, the processes of risk management and risk assessment are largely the same in military and non-military environments. Other than NIST documents, most of the IT specific risk management and assessment guidance is authored in the non-military domain. However, while the risk processes may be similar, there can be challenges with executing the activities. The difficultly arises from the size and complexity of the DoD versus business entities. The formidable task of managing risk was summed up in the 2010 QDR—"Effectively managing risk across such a vast enterprise is difficult; the range and volume of component activities and competencies defy simple identification, categorization, and aggregation of risk. Moreover, a dynamic security environment requires the Department to be flexible and diminishes the value of formulaic risk assessments" (p. 89).

Research Question 5.

What elements of continuity of operations are required to enable mission assurance? Based on the results and analysis in Chapter 4, the researcher makes the following assertions regarding the relationships of the 14 topics investigated (Figure13).

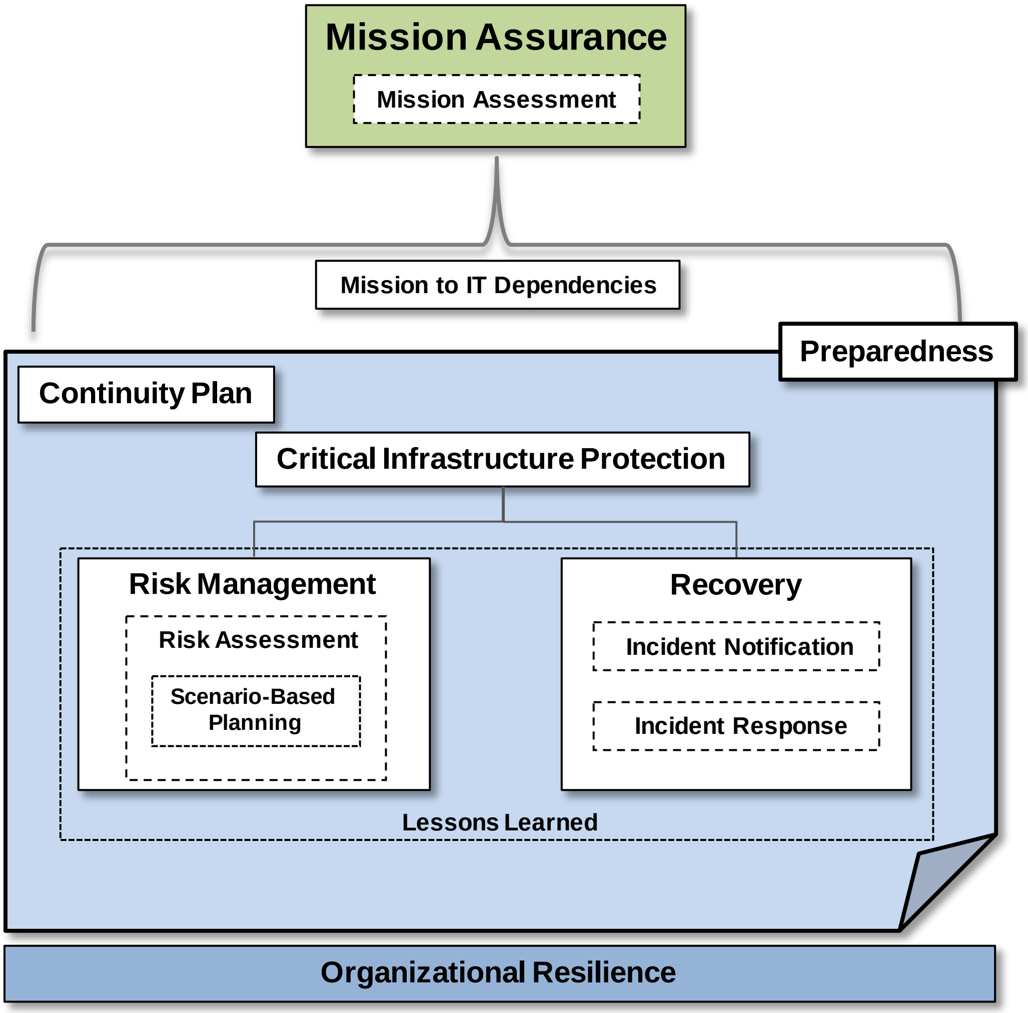

Figure 13. Relationship of 14 Topics Investigated

To explain the relationships, first consider mission assurance. Overall, the desired effect of these activities is to assure the mission. To evaluate mission success, critical success factors, mission metrics, and/or other measures must be developed. Of interest to CIMIA is the dependency on IT, particularly the identification and value of IT in respect to a mission, in support of mission assurance. As such, IT dependence is shown as one of the linkages between preparedness and assuring the mission. Mission assurance is supported by the overall concept of being prepared. Preparedness is the ability to continue operations in the event of a disaster, attack, crisis, or other disruption. To codify the concept of contingency actions or continuity of operations, plans (e.g., continuity plans, contingency plans, disaster plans, etc) are developed. The protection of critical infrastructures is supported through a risk management program and recovery procedures. Risk management includes risk assessment (i.e., the identification and assessment of risk), and risk assessments may be augmented with scenarios, such as “what if” scenario exercises. Recovery procedures include incident notification and response actions, to include learning from lessons collected and analyzed during recovery operations. These lessons learned may also be introduced into the risk management process. However, it could also be argued that lessons could be captured and learned as part of any of any organizational activities. Lastly, organizational resiliency should provide part of the foundation required for a successful preparedness culture. Organizational resilience addresses the ability to response to an incident as well as the overall style of the organization in support of adaptation to change, flexibility, etc.

The model is not all inclusive, but, captures the topics analyzed and found to be relevant to continuity of operations (i.e., preparedness). However, other risk management program activities and security-related functions (e.g., force protection, antiterrorism, and information assurance) may also help to ensure continuity of operations, and ultimately, mission assurance. Also, other terminology could be used within the model. For example, recovery, incident notification, and incident management could be summarized under “Incident Management.” The 14 labels were retained in order to provide correlation to the 14 topics analyzed in this study.

Research Question 6.

How are mission impacts represented through risk management and risk assessment to facilitate continuity of operations planning? In some of the risk management and assessment guidance, particularly with the DCIP, the guidance stressed risk-related recommendations, support information, and decisions should be coordinated between defense critical information owners and mission owners. Likewise, NIST, albeit specific to IT, proposed an organization answer two questions during IT system design—what is the purpose of the system in relation to the mission and how important is the system to the user organization's mission? These types of coordination efforts support the attempt to value resources; but, the guidance is lacking on how to represent the mission impacts. Other than limited metrics, little guidance was discovered.

Limitations of Research

This research has a few limitations. Due to the significant quantity of policies published across the DoD, only the publications available electronically on the DoD Issuances and Air Force e-Publishing web sites were included in the sample. Also, only Air Force departmental (Air Force-wide applicability) publications were included in the population. Drafts of guidance documents, i.e. policies not published yet, were not reviewed. However, while preparedness plans may be designated as "for official use only" or may be classified, and thus not included in this study, there was an expectation there should be some level of unclassified planning policy provided.

Also, researcher bias is another limitation. The researcher has been a member of the United States Air Force for over 24 years with a background in communications and information. Experience, education, and training gained over the researcher's career enabled the researcher to narrow the search parameters to relevant documents within the research domain; however, this may inject researcher bias as well. All efforts were taken to maintain objectivity and minimize bias. For example, when the researcher was selecting publications for the content analysis, key word searches were conducted during the reviews to ensure objectivity was infused into the process. However, researcher bias cannot be discounted.

Additionally, mutual exclusiveness may be a limitation to this study, specifically in regards to 2 of the 14 topics investigated—lessons learned and risk assessment. The two topics are mutually exclusive, as required for a coding measurement instrument. However, a stronger post-content analysis understanding of the topics suggested the subtopics for these two topics are potentially not mutually exclusive and could cause coding irregularities. Despite this potential limitation, the researchers remained focused by coding the text within the context of the overall category and topic.

Recommendations

Based on the content analysis conducted in this study, a few recommendations are proposed. First, the Air Force should produce an overarching continuity of operations plan matrix, or a similar umbrella matrix, linking all of the disaster, contingency, emergency, crisis, etc. plans together. NIST published a similar table in Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems (Draft),* 2009. The civil engineering community did this, in part, within the documents they authored; however, no overarching chart was discovered for all Air Force plans.

Second, in addition to a matrix, an overall continuity management plan should be authored. ITIL recommended, at the highest level, there is a need for an overall coordination plan. The Air Force does have a plan close to what is needed; the plan is the Comprehensive Emergency Management Plan (CEMP) 10-2. The CEMP provides comprehensive guidance for emergency response to physical threats resulting from major accidents, natural disasters, conventional attacks, terrorist attacks, and CBRN attacks. However, the Emergency Management Program does not cover non-physical threats, including cyber threats. As such, the CEMP should be revised to include cyberspace-related emergency management information, or a new, overarching, comprehensive emergency plan should be developed to correlate and synergize all continuity of operations efforts.

Third, there is DoD guidance directing the construction DCI mission focus statements to specify DCI performance standards and conditions necessary for mission success. However, there appears to be lack of guidance on how to implement the guidance. If the standards can be specified though, they should be able to be measured and contribute to mission metrics.

Fourth, the data suggested there is a general absence of preparedness policy authored by the communication and information community. With the previously stated importance of IT resources and assets, cyber preparedness guidance needs published to help assure mission success.

Lastly, and while this assertion needs to be supported empirically, anecdotally it appears from the researcher's 24 years of experience in the Air Force that the Air Force's ORM program is basically equated to as a safety mishap prevention program. Although ORM may be useful in preventing mishaps, ORM can be applied beyond safety. Some of this safety bias is shown in the principle ORM publication (AFPAM 90-902, *Operational Risk Management Guidelines and Tools*, 2000), as it discussed "mishap prevention," "safeguarding health and welfare," and "record low mishap rates." However, AFPAM 90-902 did go on to state, "Beyond reducing losses, risk management also provides a logical process to identify and exploit opportunities" (Department of the Air Force, 2000b, p. 5). Additional education and emphasis should be given as to how ORM should be embedded within operational processes and can be used beyond just mishap prevention.

Areas for Further Research

There are many areas associated with the overall CIMIA research project requiring additional research. However, there are a few possible areas for further research regarding the research presented.

Although the research examined DoD, Air Force, NIST, and non-governmental publications, the review was not exhaustive. Other armed services (Army, Marine, Navy) publications could be reviewed for best practice and policy discoveries to aid in the formulation of ideas and action plans to support mission assurance.

Also, while a researcher could speculate on why organizations may not perform preparedness activities (e.g., competing time/resources, lack of organizational introspection), a survey of senior leaders and/or commanders could be administered to empirically investigate this research area. For example, a survey could be conducted to determine the greatest impediments to a risk management program, the number of continuity plans developed, and the frequency of contingency plan testing and exercises.

Conclusion

This research strove to investigate the concept of mission assurance and to present a content analysis of existing continuity of operations elements within military and non-military guidance to assess the existing policy landscape to highlight best practices and identify policy gaps in an effort to further advance mission assurance by improving the timeliness and relevance of notification following a cyber incident.

The recommendations presented are just that, recommendations, and the entire CIMIA research effort is a complex challenge. However, as the dependency on IT for mission success continues to grow, cyberspace continues to become an ever increasingly contested domain, and the necessity for cyberspace situational awareness intensifies, incremental steps should be taken to enhance cyberspace situational awareness capabilities. General Eric Shinseki, former United States Army Chief of Staff, once commented, "If you dislike change, you're going to dislike irrelevance even more" (Singer, 2009, p. 254).

Appendix A: Overall Research Categories, Topics, and Subtopics

OC No.	Overall Category (OC)	Topic	Subtopics
1	Mission	Mission Assurance	- Mission Assurance - Mission Success
		Mission Assessment	- Mission Assessment - Mission Analysis - Mission Evaluation - Mission Metrics
		Mission to IT Dependencies	- Mission to IT Dependencies -- Documentation -- Governance -- Strategic Alignment/Linkages - Communications
2	Continuity Planning	Continuity Plan	- Continuity Plan - Continuity of Operations (COOP) Plan - Continuity of Government (COG) Plan - Contingency Plan - Business Continuity Plan - Crisis Management/Response Plan - Emergency Management/Response Plan - Back-up Plan - Disaster Plan - Disaster Contingency Recovery Plan
		Preparedness	- Continuity of Operations, Concept of - Continuity of Government, Concept of - Contingency Operations, Concept of - Disaster Preparedness - Emergency Preparedness - Crisis Preparedness - Readiness
		Recovery	- Recover/Restore/Remediate -- Disaster -- Disruption -- Catastrophe -- Incident
		Lessons Learned	- Lessons Learned - Impact Analysis - Business Impact Analysis - Change Impact Analysis - Impact Assessment - Impact Evaluation - Threat Analysis - Threat Assessment - Threat Evaluation
		Scenario-Based Planning	- Impact Scenarios - Worst/Likely/Best-Case Scenarios

		Organizational Resilience	- Organizational Resilience -- Organizational Commitment -- Empowerment -- Trust -- Flexibility/Adapt to Change -- Strong Organizational Foundation
		Critical Infrastructure Protection	- Critical Infrastructure Protection - Infrastructure Assurance Plan - Infrastructure Protection Plan
3	Risk	Risk Management	- Risk Management - Operational Risk Management - Enterprise Risk Management
		Risk Assessment	- Risk Assessment - Risk Evaluation - Risk Analysis - Risk Profile - Vulnerability Analysis
4	Incidents	Incident Response	- Incident Response - CNO Incident Response - Operational Incident Response
		Incident Notification	- Incident Notification - CNO Incident Notification - Operational Incident Notification

Underlined term = key search term for coding phase

Appendix B: Air Force Publication Series Number, Title and Description

(Department of the Air Force, 2006d, pp. 104-118)

Series No. and Title	Series Description
10--Operations	Publications in this series provide policy and procedures on operations, and include these subjects: **Operational readiness and security; operations** and mobilization **planning**; basing actions; capability requirements; space; support to civil authorities; civilian and foreign use of AF airfields; information operations (IO); **emergency and/or contingency planning actions and programs**; electronic warfare; **mission directives; operational reporting**; and Air Reserve Component (ARC) forces.
31--Security	These publications provide policy and procedures on the force protection of USAF warfighting resources, and include these subjects: Force protection. Weapon systems (aircraft and missiles), nuclear weapons, designated support systems, warning systems, and command and control systems. Security police, security forces activities. Law enforcement mission. **Protection of resources**. Traffic administration. Confinement, corrections, rehabilitation, and correctional custody. Use of military working dogs. Antiterrorism. Security police, security forces equipment management. Cooperation with civilian law enforcement. Off-installation enforcement. Air base defense operations (including organizing, training, and equipping organic ground defense forces). Organic USAF Point Air Defense (PAD) and Short Range Air Defense (SHORAD) operations. Prisoners of war. Classifying and declassifying classified information. Safeguarding classified information Training on classified information. Investigations, clearances, and program requirements. Industrial security. Acquisition security.
32--Civil Engineering	These publications provide policy and procedures on all aspects of Air Force Civil Engineering, including management of real property assets. They treat: Contracting, design, construction, repair, and renovation. Acquisition and transfer.

	Management and maintenance. Fire protection management. **Planning and management of contingency and wartime activities** (including all RED HORSE, Prime BEEF, Air Base Operability, and **Disaster Preparedness**). Government-owned or controlled housing used by the Air Force. Implementation of National policy goals for environmental restoration, compliance, pollution prevention, planning, and cultural and natural resource protection.
33--Communications and Information	These publications provide policy and procedures on **all aspects of communications and information management,** including command, control, communications, and computer (C4) systems that the Joint Chiefs of Staff and the Air Force use to support Department of Defense goals, managing information as a Department of Defense asset from its creation through its disposition.
90--Special Management	This series provides policy and procedure on subjects that do not more appropriately fall under one of the other AFSC-based functional series. Includes: **Organizational strategic planning.** Policy formulation. **Performance measurement.** The Inspector General. Liaison with the Congress.
91--Safety	This series provides policy and procedures on administering the Air Force Nuclear Systems Surety and Safety Programs, and includes these subjects: Monitoring, analyzing, and evaluating all phases of nuclear weapon design, operations, maintenance, modifications, and logistical movements. Preventing nuclear accidents or incidents. Overseeing ground-based nuclear reactor systems. Reviewing procedures for nuclear power systems and the space or missile use of radioactive sources. Setting safety rules for all operations with nuclear weapons and nuclear weapon systems. Identifying and eliminating hazardous practices and conditions. **Investigating and reporting mishaps.** **Creating reporting forms and procedures**. **Analyzing and evaluating mishap reports.** Recommending measures to prevent mishaps. Providing safety education. Maintaining records of statistical mishap prevention data. Ensuring flight, missile, ground, space, and explosive safety.

Appendix C: USAF Publications of Interest (Operations/10 Series)

Publication Number	Text Extracts/Notes
AFPD 10-2, READINESS, 2006	2. The Air Force will establish C2 architecture to support the Chairman, Joint Chiefs of Staff (CJCS) and combatant commanders and t**o provide continuity of C2 in the event of hostile action or natural disaster.** 6.2.4. Develop methods to **ensure continuity of operations within their commands**. 6.2.4.1. Prioritize the essential functions necessary to support mission execution and **apply risk management principals to ensure continuity.** **Continuity of Operations**—The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander.
AFPD 10-7, INFORMATION OPERATIONS, 2006	Network Operations (NetOps)—The integrated planning and employment of military capabilities to provide the friendly net environment needed to plan, control and execute military operations and conduct Service functions. NetOps provides operational planning and control. It involves time-critical, operational-level decisions that direct configuration changes and information routing**. NetOps risk management and command and control decisions are based on a fused assessment of intelligence, ongoing operations, commander‘s intent, blue and gray situation, net health, and net security.** NetOps provides the three capabilities of information assurance, network/system management, and information dissemination management. (AFDD 2-5)
AFPD 10-8, HOMELAND DEFENSE AND CIVIL SUPPORT, 2006	1.5. To fulfill the National Strategy for Homeland Security's key objectives, the DOD must have core capabilities in place to assure mission success. Mission assurance-- the certainty that DOD components can perform assigned tasks or duties in accordance with the intended purpose or plan-- is therefore itself a key objective. DOD's framework for mission assurance includes a range of programs and efforts aimed at securing DOD warfighting capabilities even when under attack or after disruption. These include force protection measures, installation preparedness, COOP, emergency management (EM), consequence management, **continuity of government (COG)** and critical defense infrastructure protection. 6.2.4. Maintain a comprehensive and effective **COOP and CIP to ensure continuity of mission essential functions** under all circumstances.

AFPD 10-24, AIR FORCE CRITICAL INFRASTRUCTURE PROGRAM (CIP), 2006	1. Air Force operations in support of the National Military Strategy are dependent on globally linked physical and cyber infrastructures (US and foreign, public and private sector). These interconnected infrastructures, while improving capabilities and mission effectiveness, also increase the Air Force's vulnerability, in regards to failures due to human error, natural disasters, and/or intentional attack. Consequently, it is important to identify and protect those infrastructures that are truly critical to the Air Force so it can accomplish its worldwide missions. 3. The Air Force CIP will complement and integrate the **mission assurance aspects of existing Air Force** Antiterrorism, Force Protection, Information Assurance, **Continuity of Operations, and Readiness programs.** 4. It is the Commanders' responsibility to **judiciously manage risk in order to accomplish the mission.** 5.2. The Secretary of the Air Force, Communications (SAF/XC dual-hatted as A6): 5.2.3. Plans and develops procedures to **ensure continuity of operations for information systems that support the operations and assets of the Air Force**. 6.7. Monitor and report decisions undertaken to remediate identified **critical asset vulnerabilities**. In case of loss or disruption of critical infrastructure, develop strategies for mitigating the effects of such loss or disruption and include them in the **Continuity of Operations Plans (COOP)**. **Critical Infrastructure Asse**t—An infrastructure asset deemed essential to Air Force operations or the functioning of a Critical Asset. **Critical Infrastructure Program (CIP)**—The identification, assessment, and **security enhancement of cyber and physical assets** and associated infrastructures essential to the execution of the National Military Strategy. It is a complementary program linking the mission assurance aspects of the Anti-Terrorism, Force Protection, Information Assurance, **Continuity of Operations**, and Readiness programs. **Critical—**The level of **importance of an asset to the success** of the Combatant Commands or Air Force mission. For the AF CIP, criticality is broken down into four Tiers: – Tier I - Warfighter/Combatant Commands suffers strategic mission failure. Specific timeframes and scenarios assist in infrastructure prioritization. – Tier II - The Air Force suffers mission failure, but warfighter strategic mission is accomplished. – Tier III - Individual element failures, but no debilitating strategic or Air Force mission failure. – Tier IV - Everything else.
AFPD 10-25, EMERGENCY MANAGEMENT, 2007	3. Air Force o**rganizations will use** the **AFIMS for peacetime and wartime incident response and recovery**. The Air Force will support federal emergency preparedness and incident management programs consistent with military operations. EM Program policies, guidance and procedures will focus on operational requirements and will incorporate requirements in the National Response Plan, federal statutes, DOD guidance and host-nation agreements. **Critical Infrastructure Protection—Mission Assurance/Risk Management program** involving actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on risk, these actions could include changes in tactics, techniques or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding; or similar measures. (DODD 3020.40)

AFI 10-201, STATUS OF RESOURCES AND TRAINING SYSTEM, 2006	Wartime Mission—A task or group of tasks assigned to a unit in an approved operations plan and expected to be executed during some level of armed conflict whether incident, limited war, or general war. 1.1.3.3. A fundamental premise of **SORTS reporting** is integrity. Commanders must "tell it like it is" (in accordance with (IAW) paragraphs 1.10.7. and 1.10.8.) and not allow masking of deficiencies to affect their ability to provide capability or other readiness related information. **Risk must be balanced with responsibility.** Effective management of unit resources requires accurate information at all levels.
AFI 10-204, PARTICIPATION IN JOINT AND NATIONAL EXERCISES, 2010	Exercises play an essential role in preparing United States Air Force (USAF) forces to conduct air, space, and cyberspace operations and perform their mission essential tasks. 1.5.4.1.2. **Ensure exercise activities help** command and subordinate units achieve and maintain their designed operational capability, and are able to fulfill OPLAN taskings and **appropriately respond to contingencies, such as natural disasters or terrorist incidents.**
AFI 10-206, OPERATIONAL REPORTING, 2008	3.1. Subject and Purpose. CPs uses the OPREP-3s to immediately notify commanders of any **significant event or incident** that rises to the level of DoD, AF, or MAJCOM interests. Subject of OPREP-3 (reference event/incident category from AFI 10-206, Attachment 2, OPREP-3 and Reports Matrix). Aircraft/equipment status (available, fully mission capable, partially mission capable, not mission capable)
AFI 10-207, COMMAND POSTS, 2008	6.1. Mission Movement. Execution of the mission is accomplished by controllers performing pre-flight, in-flight, and post-flight coordination, direction, and **reporting necessary to ensure successful mission accomplishment for all tasked missions**. 6.1.1. Mission management is the function of organizing, planning, directing, and controlling Combat Air Forces (CAF), MAF, and training missions operating worldwide. Mission management includes mission execution authority: the authority to direct where and when a mission goes and what it does once it arrives. This function is typically performed at the AOC level. An example of mission management is the Tanker Airlift Control Center (TACC). **Mission Management**—The function of organizing, planning, directing, and controlling AMC airlift and/or tanker mission operating worldwide. Mission management includes mission execution authority, the authority to direct where and when a mission goes and what it does once it arrives there. The TACC and AME controllers are mission managers.
AFI 10-208, CONTINUITY OF OPERATIONS (COOP) PROGRAM, 2005	Chapter 1— DEPARTMENT OF THE **AIR FORCE COOP POLICY AND GUIDANC**E 1.1. General; 1.2. Air Force Guidance; 1.3. Air Force Policy; 1.4. Air Force Organizational Responsibilities; 1.5. Air Force Organizational Responsibilities for a COOP Program; 1.6. Air Force Organizational Responsibilities for COOP Planning; 1.7. Air Force Organizational Responsibilities for COOP Training; 1.8. Air Force Organizational Responsibilities for COOP Exercises; 1.9. Air Force Organizational Responsibilities for COOP Communication and Logistics; 1.10. Air Force Organizational Responsibilities for COOP Funding and Acquisition; 1.11. Air Force Organizational Responsibilities for COOP Issue Resolution Chapter 2— **COOP PLAN DEVELOPMENT GUIDANCE** 2.1. COOP Planning Factors; 2.2. Implementing COOP Plans; 2.3. Writing the COOP Plan; 2.4. Classifying COOP Plans; 2.5. COOP Plan Review. All organizations are required to validate and update their COOP plan every 2 years Chapter 3— **HAF COOP PROGRAM.** 3.1. Introduction; 3.2. Applicability; 3.3. HAF Responsibilities; 3.4. Additional Tasked Organizations; 3.5. Emergency Planning Coordinator Responsibilities; 3.6. Air Force Emergency Operations Center (AFEOC) and Site M Administration; 3.7. Exercises and

	Training; 3.8. Issue Resolution
AFI 10-209, RED HORSE PROGRAM, 2008	1.5.1. Establish a command RED HORSE program to ensure personnel are **organized, trained, and equipped to respond to wartime, disaster, and other contingency-related missions**. **Contingency**—An emergency involving military forces caused by natural disasters, terrorists, subversives, or military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response, and special procedures to ensure the safety and readiness of personnel, installations, and equipment.
AFI 10-211, CIVIL ENGINEER CONTINGENCY RESPONSE PLANNING, 2008	Chapter 2— **CONTINGENCY RESPONSE PLANNING** AND PREPARATIONS 2.1. Peacetime Planning; 2.2. Disaster and Attack Preparations; 2.3. Disaster Recovery Tasks Chapter 3— **CE CONTINGENCY RESPONSE TEAMS** 3.1. Command and Control (C2); 3.2. CE Contingency Response Structure; 3.3. Military Personnel; 3.4. Civilian Personnel **Contingency**—An emergency involving military forces caused by natural disasters, terrorists, subversives or by required military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response and special procedures to ensure the safety and readiness of personnel, installations and equipment. **(JP 1-02)**
AFI 10-213, COMPTROLLER OPERATIONS UNDER EMERGENCY CONDITIONS, 1994	2.4.1. Ensure their command or agency comptroller wartime and contingency planning is accomplished per applicable guidelines, including those in the comptroller annexes to the WMP, the **USAF Survival, Recovery, and Reconstitution (SRR 355) Plan**, AFPD 10-4 and AFMAN 10-401 and AFIs 10-402, Mobilization Planning, and 10-403, Deployment Planning, and this instruction. 7.4. Contingency Plans. 7.4.1. There are numerous scenarios that could occur at a base-level comptroller office which would affect the mission. **Every base has some risks uniquely associated to location, weather, or mission.** Each base level comptroller office is **tasked with developing and maintaining local plans to be implemented in the event of a local emergency or natural disaster. S**pecific guidance is contained in AF 170, 172, and 177 series publications and AFI 32-4001. Comptroller personnel should work closely with disaster preparedness personnel to develop the plans. These plans should cover, as a minimum, the following: 7.4.1.1. The roles of the accounting and finance office (DAO and FSO), and the financial analysis office. 7.4.1.2. Points of contact at all levels in the event of implementation of the plan. 7.4.1.3. Priority mission requirements. 7.4.1.4. Guidance for implementation.
AFI 10-218, PERSONNEL ACCOUNTABILITY IN CONJUNCTION WITH NATURAL DISASTERS OR NATIONAL EMERGENCIES, 2006	1.1. Background. During natural disasters or national emergencies, the ability to **quickly assess the status of Air Force Airmen**, Department of the Air Force (DAF) and Nonappropriated Funds (NAF) civilians and families is critical. Both our **ability to recover from these incidents** and to return to normal operations are top priorities.

AFPAM 10-219V1, CONTINGENCY AND DISASTER PLANNING, 2008	2.4.2. **Comprehensive Emergency Management Plan (CEMP) 10-2**. At any USAF base, the CEMP 10-2 is the "master" plan for base level emergency response to physical threats resulting from major accidents; natural disasters; enemy attack or terrorist use of chemical, biological, radiological, nuclear or high-yield explosives (CBRNE). This plan outlines actions and assigns responsibilities to agencies required to cope with catastrophes caused by the incidents mentioned above—especially those that involve nuclear or other hazardous material. This can be a very useful and versatile document. A planner can add appendices to the annexes to cover almost any disaster. A few other plans are often incorporated in this way. Civil engineers are responsible for preparing this plan, but it requires the input of many other organizations on base. This plan helps provide the basis on which to build the CE Contingency Response Plan. The directing document for the CEMP 10-2 is AFI 10-2501, Air Force Emergency Management (EM) Program Planning and Operations. This publication lays out the basic requirements; however, the MAJCOM may provide additional details. 6.5.1. **Set Objectives.** When planning CE inputs, first determine or set objectives for the exercise. **The particular crisis or threat will dictate the basic thrust of the exercise.** Also consider MAJCOM special interest items, Inspector General (IG) findings from other units, and deficiencies noted from previous exercises when setting exercise objectives. Do not overlook the common-core criteria detailed in AFI 90-201, Inspector General Activities. General information is also contained in AFI 10-204, Readiness Exercises and After-Action Reporting Program. Obviously, the scenarios should test response capabilities and evaluate response planning. Scenarios should also identify limiting factors (LIMFAC) and evaluation of the following: 6.5.1.1. Recall procedures. 6.5.1.2. Command and control. 6.5.1.3. Crisis management; the ability to respond to the situation (recovery actions). 6.5.1.4. Predisaster actions. 6.5.1.5. Security (OPSEC and COMSEC). 6.5.1.6. Deployment processing. 6.5.1.7. Postdisaster recovery. A3.2.4.2. **Vulnerability Analysis.** Identify the parts of the base or off-base community that may be affected by each hazard or threat; the population within each zone that is subject to harm; critical facilities or functions at risk (for example, hospital and command post); and property and environmental systems that may be damaged. A3.2.4.3. **Risk Analysis.** A risk analysis provides a means to judge the relative likelihood of a hazard/threat occurring and the magnitude of harm to personnel and mission should that hazard/threat occur.

AFPAM 10-219V2, CIVIL ENGINEER DISASTER AND ATTACK PREPARATIONS, 2008	3.5.3.4. **Dispersal During Survival, Recovery, and Reconstitution (SRR) Plan** Implementation. The SRR plan is intended to improve survival and **enhance recovery and reconstitution operations** for CONUS air force installations under threat of nuclear attack. Not all CONUS civil engineer units have responsibilities under an SRR plan. For those installations that do, the BCE and staff should carefully review the local SRR plan to determine specific actions required during implementation. The general SRR concept of operations during various attack phases follows. 4.2.1. **Emergency Operations Center (EOC).** The EOC is the C2 support element that directs, monitors, and supports the installation's actions **before, during, and after an incident, attack, or disaster.** 4.4.1.2. **Incident Status Displays.** In addition to maps, readily visible status displays (usually electronic or status boards) help the EOC staff keep track of the condition of the installation, unit status, and the recovery efforts. Suggested incident status displays include those listed in Table 4.3. 4.4.4. **Continuity of Operations.** Provide for continuity of command and control. Organize the second shift for the control center. Set up an alternate control center during wartime operations. There are many ways to do this. 7.2.3. **Risk Analysis.** Risk analysis is an assessment of the likelihood of an accidental release of a hazardous material and the consequences that might result based on the estimated vulnerable zones. Risk analysis is based on the history of previous incidents at the installation, mathematical modeling, and the best available information. 8.1. Introduction. Support between units is a routine activity at most air bases and is necessary to ensure daily mission accomplishment. Likewise, the support that **CE provides to and receives from others during or after an emergency also helps to ensure mission continuity**.
AFPAM 10-219V3, CIVIL ENGINEER DISASTER AND ATTACK RECOVERY PROCEDURES, 2008	1.1. General Information. The **unpredictable nature of war and disasters requires a great degree of flexibility** by the civil engineer (CE) force during disaster and attack recovery operations. CE units must maintain **contingency response capabilities to restore operations**, save lives, mitigate human suffering, and minimize damage during and after a crisis on or near the installation. The **CE contingency response plan (CRP)** should be followed to ensure a coordinated response; however, no plan covers all possible scenarios. Therefore, all elements of the civil engineer team must have the ability to quickly adjust to changing circumstances. Engineering knowledge, experience, and common sense are crucial factors to installation recovery. Immediately after a disaster or attack, civil engineers operate in the reactionary mode to immediately eliminate life-threatening hazards. In later phases of the recovery, the engineer force begins a more deliberate effort. The environment may still be chaotic and there are still many immediate actions that must be taken, but the overwhelming dangers that prevailed during the emergency are past. The effort to identify and quantify the damage, assign repair priorities, and determine recovery strategy now begins. Volumes 1 and 2 of this pamphlet series discuss preparedness planning and steps to take prior to experiencing a natural/manmade disaster or installation attack. This volume, coupled with Volume 4, Airfield Damage Repair Operations, provide CE procedures that form the basis for an effective installation recovery capability. 2.3.4.1. **Recovery Activities.** The EOC determines the scope of the damage and its impact on the installation mission. The EOC accounts for personnel and casualties and monitors material resources. It develops a **recovery strategy**, directs recovery actions, and tracks recovery progress.

AFPAM 10-219V4, AIRFIELD DAMAGE REPAIR OPERATIONS, 2008	1.4.7.8. **Airbase Recovery.** Forces must be prepared to recover the airbase after a conventional attack with the resumption of flying operations as first priority. **Other recovery activities may be conducted concurrently;** however, these activities must not impede the resumption of flying operations. Base recovery actions should be identical whether at a MOB or bare base. 2.1. General. **Mission success** in all theaters of operation depends upon the level of individual and unit training.
AFPAM 10-219V7, EXPEDIENT METHODS, 2008	2.1. Introduction. **Expedient construction** and repair of roads and drainage systems **during disasters or after an attack could be crucial to recovery operations** and mission sustainment.
AFPAM 10-219V8, PRIME BASE ENGINEER EMERGENCY FORCE (BEEF) MANAGEMENT, 2007	1.3. **Military Operations Planning**. Good operations planning enables the Air Force—jointly with its sister services—to respond rapidly and effectively to anticipated threats or unforeseen crises. Because many of the concepts and terms used in this volume are tied to joint operations planning, this short over view of military operations planning is included to help clarify the process unfamiliar to many personnel. For more details, see AFI 10-401, Air Force Operations Planning and Execution. 1.3.1. **Deliberate Versus Crisis Action Planning.** Operation planning is usually done deliberately during peacetime to **prepare for likely threats**; however, operation planning is done in the **crisis action mode when an unanticipated crisis arises with little or no warning**. The big difference between deliberate and crisis action planning is the amount of time available. In the crisis action mode, the situation will dictate whether **commanders and planners can modify a deliberate plan or must create a "no plan" response.** 1.3.2. **Operation Plans.** In either case, operation planning is a process to determine how to **respond to a likely threat or actual crisis** and what forces are needed. The result is documented in an operations plan (OPLAN) or, if time is very short, in the operations order (OPORD). An OPLAN or OPORD identifies which combat and support units will be used to respond to the threat or crisis. It shows where, when, and how those forces will be deployed, employed, and supported. An OPLAN also outlines the command structure and provides functional area direction. An OPLAN covers the five phases of a military operation: mobilization, deployment, employment, sustainment, and redeployment. Major OPLANs are updated every 24 months. 1.4. **The next few paragraphs highlight key parts of the systems and subsystems that affect civil engineers. For more information on these systems, refer to AFI 10-401.** 2.8.5.8. Create the force beddown or **base recovery plan of action.** Clearly define the tasks for subordinates and make sure they understand their tasks, resources, and required completion times. Ensure the latest available data, plans and checklists are being utilized for beddown/recovery plans. Verify through appropriate personnel/offices/directorates.

AFH 10-222V3, CIVIL ENGINEER GUIDE TO EXPEDITIONARY FORCE PROTECTION, 2008	1.3. Elements of Force Protection. Force protection includes efforts designed to prevent attacks on DOD assets and interests and minimize the effect of any attacks. It is unrealistic to assume every DOD asset can be protected. For this reason, **plans and preparations to recover from an attack must be focused on enabling the mission to continue and restoring confidence** throughout the unit and local population. 1.3.4. Recovery. **Commanders design plans to recover from the effects of a terrorist incident while continuing the mission.** Air Force emergency man-agement procedures are outlined in AFI 10-2501, Air Force Emergency Management (EM) Program Planning and Operations. 2.7. **Risk Management.** Risk management is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions to balance risk costs with mission benefits. This process is called a risk assessment. Risk assessments provide commanders with a method to assist them in making resource allocation decisions designed to protect their personnel and assets from possible terrorist threats in a resource-constrained environment. The risk assessment is based upon three critical components: threat, criticality, and vulnerability assessments. It is conducted after completing all other assessments. Any plan that does not start with these assessments will probably be too reactive and result in wasted efforts and resources. Once vulnerabilities are identified, commanders manage risk by developing strategies to deter terrorist incidents, employing countermeasures, and mitigating the effects and developing plans to recover from terrorist incidents. Civil engineers participating in the development of FP and AT plans should also participate in the risk assessment. The information collected during the risk assessment is critical to developing effective FP and AT plans. For more information on risk management, refer to **AFTTP(I) 3-2.34, Multi-service Tactics, Techniques, and Procedures for Risk Management.** **5.2.1. Assessment. As stated in Chapter 2, an assessment of the threat, including vulnerability, criticality, and risk assessments, must be conducted to determine how best to employ defensive measures.**
AFH 10-222V4, ENVIRONMENTAL GUIDE FOR CONTINGENCY OPERATIONS, 2007	2.1.1. **Risk Management.** Risk Management is an effective method for ensuring all environmental concerns are addressed. Environmental risk management matrices can be used to identify when, where, and how planned training activities or fast-paced military operations might cause damage to the environment and to what extent. Plans can then be adjusted to minimize adverse effects on the environment and personnel without jeopardizing the mission. This increases the overall chance of mission success. 2.2.5. **Risk Assessment (RA).** A Risk Assessment (RA) is normally included in the EIAP and can be conducted prior to operations to determine potential environmental impacts. The RA can be used to assess alternative methods or actions which might minimize environmental impacts. The RA is also used to determine the level of acceptable risk in the contingency environment when operations take priority.
AFH 10-222V8, GUIDE TO MOBILE AIRCRAFT ARRESTING SYSTEM INSTALLATION, 2006	1.2.2.1. Based on the above information, the Wing or Installation Operations Center should pass information through the **Survival Recovery Center (SRC)** or the **CE disaster control center (DCC)** in order to make appropriate MAAS installation, operation, and maintenance decisions.

AFH 10-222V14, CIVIL ENGINEER GUIDE TO FIGHTING POSITIONS, SHELTERS, OBSTACLES, AND REVETMENTS, 2008	1.3.1. **Planning Factors.** Some key factors engineers consider while planning for physical security include desired levels of protection, potential threats, criticality and vulnerability assessments, and acceptable levels of risk. 1.3.2. Levels of Protection. Physical security measures are employed to obtain certain levels of protection. These protection levels are usually based upon known threats and the results of intelligence and assessment reports. It is unrealistic to believe all assets can be protected and the threat completely eliminated. This perception causes valuable resources to be wasted or misallocated. Risk management is based on the assumption that some risks must be taken to ensure limited resources are applied against the highest priority assets first, rather than all assets equally. Criticality assessments usually result in the assignment of certain values to particular assets. **They reveal the degree of debilitating impact that destruction of certain assets would have upon the mission;** obviously, personnel come first. **Unacceptable losses require higher levels of protection.** Assets most critical to the mission must be afforded higher levels of protection, especially if vulnerability assessments indicate these assets are not already sufficiently protected. Different levels of protection are described in UFC 4-020-01, DOD Security Engineering Facilities Planning Manual. The following paragraphs cover the assessments usually conducted to assist commanders in determining levels of protection. 1.3.3. **Threat Assessment.** This assessment is used to identify threats based on key factors such as the existence, capability, and intentions of potential hostile forces and terrorist groups. Group activities and the operational environment are also considered. Potential threats are categorized in various ways (e.g., terrorists, saboteurs, spies, extremists, criminals). Any weapons, tools, and explosives likely to be used in an attack upon DOD personnel or critical assets are also identified during the assessment. 1.3.5. **Vulnerability Assessment.** The vulnerability assessment is an evaluation conducted to determine if key assets are provided appropriate levels of protection. Protection levels are based on minimum standards where no specific threat has been identified or on higher levels of protection where a specific threat has been identified. This assessment analyzes the threat, likely tactics, and key targets that may be vulnerable to attack. 1.3.6. **Risk Assessment.** Risk assessments help commanders make decisions on the most effective ways to allocate limited resources needed to protect personnel and critical assets. The assessment is based upon the results of the threat, criticality, and vulnerability assessments. Based on these assessments, the commander commits resources to achieve certain levels of protection for personnel and mission-critical assets. With limited resources, all assets cannot be afforded equal levels of protection. **Risk Management provides the commander with the best information available to make resource allocation decisions.** If plans do not incorporate these assessments, they will likely be too reactive and cause limited resources to be misdirected or wasted. For additional information on the assessments used in determining levels of protection, refer to AFH 10-222, Volume 3, Civil Engineer Guide to Expeditionary Force Protection. **Risk Management**—The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits.
AFH 10-222V16, GUIDE FOR USE OF THE MINIMUM AIRFIELD OPERATING SURFACE MARKING SYSTEM, 2005	The expedient procedures in this handbook are **emergency recovery action**s performed when urgent mission requirements and i**nsufficient time prevents restoring the markings to their original peacetime criteria.**

AFH 10-222V22, REFUGEE CAMP PLANNING AND CONSTRUCTION HANDBOOK, 2000	Flexibility. Another likelihood during a refugee crisis is that “firm” requirements will often change. **Like any contingency operation, critical planning factors that are unknown during the planning stage can have significant impacts on the project as the operation progresses**.
AFI 10-245, ANTITERRORISM (AT), 2009	1.1.2. AT programs should be coordinated with overarching efforts to achieve protection, such as Force Protection (FP), **critical infrastructure protection and continuity of operations**, as described in Joint Publication (JP) 3-07.2, Antiterrorism. 1.2.14.3. Implement terrorism **incident planning for response, consequence management and recovery** within AT Programs. 2.20.1. Incident response measures shall be developed consistent with the principles outlined in DOD 5200.08-R and AFI 10-2501 and included in the overall AT plan. These measures shall include procedures for determining the nature and scope of incident response (including incidents with a CBRNE component); procedures for coordinating security, fire, medical, hazardous material and other emergency responder capabilities; and **steps to recover from the incident while continuing essential operations.** **AT Risk Management**—The process of systematically identifying, assessing and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. The end products of the AT program risk management process shall be the identification of DOD elements and personnel that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT **risk management** (threat assessment, criticality assessment and vulnerability assessment), the commander must determine which DOD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate or prepare for a terrorist incident. Table 2.1. AT Threat **Planning Scenarios**. Figure 2.1. AT **Risk Management Process**. A4.1. Overview . The commander has an inherent command responsibility to reduce risks that threaten the mission with available resources. **Risk management described in AFPD 31-1, aids the commander in assessing risk**.
AFI 10-246, FOOD AND WATER PROTECTION PROGRAM, 2004	2.28.8. Develops **contingency support plans** and **base recovery actions** related to water systems IAW applicable AF policy and coordinates plans/actions with appropriate base agencies. Attachment 3 - Operational Risk Management (ORM)
AFI 10-401, AIR FORCE OPERATIONS PLANNING AND EXECUTION, 2006	**Risk**—1. Probability and severity of loss linked to hazards. 2. See degree of risk. See also hazard; risk management. **Risk Assessment**—(DOD) The identification and assessment of hazards (first two steps of risk management process). **Risk Management**—(DOD) The process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits. Also called RM. See also risk.

AFMAN 10-401V2, PLANNING FORMATS AND GUIDANCE, 1998	3. ( ) EXECUTION [C4 INFORMATION SYSTEMS PROTECTION(U)] a. ( ) **Concept of Operations.** Summarize the description of the environment, intended use, and broad security guidance. Include personnel clearance and access levels, the sensitivity assessment, security mode of operation, and both hardware and software security mechanisms and identify all intended connections and interfaces. Employ information protection tools, **backups/recovery, and other procedures or tactics to thwart adversary lethal and nonlethal attacks on friendly C4 information systems.** Include low system threats, vulnerabilities, and **countermeasures are to be obtained and degrees (low, medium, high) of assurance for availability, integrity, confidentiality, and accountability.** **b. ( ) Tasks.** Identify a command element that is responsible for coordinating C4 information systems protection actions. In separate sub-paragraphs, assign tasks and responsibilities to each subordinate command in order to implement and accomplish C4 information systems protection actions (to include identifying C4 information systems protection vulnerabilities). **Develop emergency recovery procedures in the event all protection measures fail.**
AFI 10-403, DEPLOYMENT PLANNING AND EXECUTION, 2008	2.23. Factors in Determining **Worst-Case Scenario**. 2.23.1. There are a number of factors units must consider in **estimating their worst-case scenario**. The IDO works with functional planners, unit representatives, operational planners, and MAJCOMs to determine the worst-case scenario. They review contingency plans the installation is tasked to support, the UTC Availability, UTC availability P-coding, DOC statements, home station mission requirements, possible installation through-put, etc. Table 2.1. depicts many of the factors that must be considered.
AFI 10-420, COMBAT AIR FORCES AVIATION SCHEDULING, 2006	4.2.2. All **MAJCOM objections must be stated in terms of the four GFM risk categories**: operational risk, force management risk, future challenges risk, and institutional risk. For CAF SIPT purposes, force management risk is the most likely category. **Risk Definitions** Operational Risk: The ability to achieve military objectives in a near-term conflict or contingency. Future Challenges Risk: The ability to invest in new capabilities and develop new operational concepts needed to dissuade or defeat mid- to long-term military challenges. Force Management Risk: The ability to recruit, retain, train, and equip sufficient numbers of quality personnel and sustain the readiness of the force while accomplishing its many operational tasks. Institutional Risk: The ability to develop management practices and controls that use resources efficiently and promote the effective operation of the Defense establishment. **Risk Levels** Low Risk: Success can be achieved with planned resources; unanticipated requirements can be easily managed with minimal impact on the force. Moderate Risk: Success will require additional resources from other plans or operations; timelines will have to be extended to achieve commander's end states; unanticipated requirements may necessitate adjustment to the plan. High Risk: Success will require resources from other plans and operations and some significant capability shortfalls may exist; significant adjustments to timelines will be required; unanticipated requirements will necessitate major adjustments to plans. Extreme Risk: Success will require extraordinary adjustments to plans and programs; will require reallocating significant resources from other operations; some resources may be deficient or absent altogether; even with significant adjustments to timelines, all commander's objectives may not be achieved; the force will be unable to manage unanticipated requirements.

AFI 10-604, CAPABILITIES-BASED PLANNING, 2006	**Capabilities-Based Planning**—Planning, under uncertainty, to provide capabilities suitable for a wide range of challenges and circumstances, all designed to achieve certain battlespace effects. **Capabilities Review and Risk Assessment (CRRA)**—A process identifying Air Force-wide capability shortfalls, gaps, and tradespace study areas. Capabilities review, risk assessment, and senior leader review and decisions are incorporated into the CRRA process. **Course of Action**—1. Any sequence of activities that an individual or unit may follow. 2. A possible plan open to an individual or commander that would accomplish, or is related to the accomplishment of the mission. 3. The scheme adopted to accomplish a job or mission. 4. A line of conduct in an engagement. 5. A product of the Joint Operation Planning and Execution System concept development phase.
AFI 10-701, OPERATIONS SECURITY (OPSEC), 2007	2.1.1. OPSEC is accomplished using a five-step process: 1) Identify critical information; 2) **Analyze threats; 3) Analyze vulnerabilities; 4) Assess risk**; and 5) Apply OPSEC measures. Although these steps are normally applied in a sequential manner during deliberate or crisis action planning, dynamic situations may require any step to be revisited at any time. **Acceptable Level of Risk**—An authority's determination of the level of potential harm to an operation, program, or activity due to the loss of information that the authority is willing to accept.
AFI 10-802, MILITARY SUPPORT TO CIVIL AUTHORITIES, 2002	1.2. Homeland Security (HLS). The preparation for, prevention of, deterrence of, preemption of, defense against and response to threats and aggressions directed towards US territory, sovereignty, domestic population, infrastructure; as well as **crisis management, consequence management**, and other domestic civil support. HLS includes domestic preparedness, critical infrastructure protection, and civil support in case of attacks on civilians, **continuity of government, continuity of military operations**, border and coastal defense, and national missile defense. MSCA operations are a part of the nation's Homeland Security campaign.
AFI 10-901, LEAD OPERATING COMMAND--COMMUNICATIONS AND INFORMATION SYSTEMS MANAGEMENT, 2001	3.7.12. Ensures **operational risk management (ORM) is incorporated into the Lead Command process** in accordance with Air Force Pamphlet (AFPAM) 91-215, Operational Risk Management (ORM) Guidelines and Tools, to help control risks.
AFI 10-1211, SPACE LAUNCH OPERATIONS, 2006	1.2. S**pace and Missile Systems Center (SMC)** is the AFSPC organization responsible for acquisition and sustainment of the Expendable Launch Vehicle flight systems and ground systems. **SMC performs** acquisition management **and mission assurance** for these systems. **Mission Assurance**—Accomplished through the contractor's demonstration of their production, operation, maintenance, and problem resolution processes with government personnel performing surveillance to ensure these processes result in an acceptable level of mission risk to the government.

AFI 10-1212, SPACE LAUNCH VEHICLE RETURN TO FLIGHT, 2001	2. Scope. This instruction applies to all (government and commercial) unmanned space launch vehicle systems (current and future) that have a launch mishap at an AFSPC space launch range, or have commonality to another system that has a mishap. There are two RTF certification processes: safety assurance and **mission assurance**. 3.2. **Mission Assurance RTF Certification Process.** Mission assurance certification demonstrates that appropriate corrective actions have been taken to ensure mission success. Responsible agencies will actively participate in the mission assurance RTF process by providing the SMC/CC and SW/CC with an analysis, an action plan and written certification that mission assurance RTF criteria have been met. For USAF-supported missions, the SMC/CC will approve mission assurance RTF certification as soon as it is complete, but no later than the FRR for the first flight following a launch mishap for the affected launch system. If mission assurance RTF certification is not complete by the scheduled FRR, the FRR and possibly the launch will be rescheduled to a later date. 4. Criteria. Safety and **mission assurance RTF certificatio**n will determine the readiness to resume flight operations for a space launch vehicle system based on the following criteria. **4.2. Mission Assurance Criteria.** The SMC/CC is responsible for certifying that mission assurance criteria are met for USAF-supported missions. As a minimum, certification must address the following criteria: 4.2.1. Ensure all failure-related issues involving pre-launch processing are resolved. 4.2.2. Ensure all failure-related issues involving launch vehicle and/or payload performance go/no-go criteria are resolved. 4.2.3. Ensure all failure-related issues involving launch vehicle and/or payload hardware production, integration and test, vehicle inspection/checkout, or contractor processes/procedures are resolved. 4.2.4. Ensure all failure-related issues involving launch vehicle and/or payload design flaws are resolved.
AFI 10-2001, DEFENSIVE COUNTERINFORMATION PLANNING, OPERATIONS AND ASSESSMENT, 2001	1.2. Defensive Counterinformation (DCI) involvement should incorporate an operational risk management (ORM) process by which commanders assess and address risks posed to their information and associated infrastructures. In order to achieve these goals, **commanders and planners must identify mission critical information and information systems, conduct vulnerability assessments on those systems, develop and implement plans to mitigate risk,** include these activities in exercise planning and implementation, and include DCI considerations into the acquisition and procurement planning cycles. 2.1.1.2. Ensure operational and exercise planning includes identification and **risk assessment of friendly information centers of gravity (COGs).** 2.1.1.3. Integrate Operational Risk Management (ORM) to develop courses of action to mitigate vulnerabilities of these critical friendly information COGs. See AFI 90-901, Operational Risk Management (ORM). 2.1.1.4. Periodically test an organization's ability to protect information COGs via the unit's exercise program.
AFI 10-2303, BATTLELABS, 2003	2.4. **Knowledge Management.** Maintaining an accessible repository for accumulated knowledge is crucial for exchanging information among innovation organizations, activities, and stakeholders. HQ USAF/XIIV maintains the Information Sharing Website (ISW) to facilitate the exchange of information. The ISW is comprised of resources, Public Affairs information, **lessons learned**, summaries of initiatives, and AIRs. The ISW (a restricted website) can be found at (https://www.battlelabs.hq.af.mil/). 2.4.1. **Lessons Learned.** Significant impacts to the planning and/or execution of each Initiative will be documented in a lessons learned database maintained by HQ USAF/XIIV in the ISW to insure best practices are followed to the maximum extent possible. Significant

	impacts include any major cost, schedule, or safety factors that were avoided, or could have been avoided by taking additional planning or execution steps. **Course of Action (COA)**—A step-by-step plan to accomplish a goal with the following elements: 1) strategy to achieve; 2) methods of measurement; 3) schedule and **risk;** 4) funding required; 5) expertise required; and, (6) organizational support required.
AFI 10-2305, WARGAMING, 2003	3.1.4.1. Plan and conduct the Air Force Future Capabilities Wargame (FG) series of **wargames.** All facets of wargame planning, execution, and post-game activities will be under the **direction and guidance of HQ USAF/XPX**.
AFI 10-2501, AIR FORCE EMERGENCY MANAGEMENT (EM) PROGRAM PLANNING AND OPERATIONS, 2007	3.3.4.10. Assesses operational impact of attacks on air bases; identifies key enablers for mission recovery and sustainment; and develops and **tests risk-based mitigation strategies** for commanders. 4.5. **Standard Phases of Incident Management**. The NIMS and the NRP state that the five phases of incident management are prevention, preparedness, response, recovery and mitigation. These phases of incident management have been incorporated into AFIMS and provide the framework with which the installation DRF responds to all EM events. Comprehensive definitions of these phases are included in Attachment 1. 6.6.11. The **Air Force Incident Management Course** (formerly the On-Scene Commander's Course) is an Air Force-unique course for EOC Directors, their alternates and EOC Managers. 6.6.5.2. AERO – Command and Control (C2) Course. This course incorporates the AERO Introduction Course and describes Air Force Emergency Response Operations with an emphasis on **command and control during incident response and recovery**. 8.4. **After-Action Reports.** Procedures for after-actions reports are provided in AFI 10-204. Commanders must send an installation-wide lessons-learned report to their MAJCOM, FOA, or DRU for all emergency responses. After-action reports should include actions implemented and any lessons learned during actual incident response and exercises. **Contingency**—An emergency involving military forces caused by natural disasters, terrorists, subversives, or by required military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response and special procedures to ensure the safety and readiness of personnel, installations, and equipment. **Contingency Operations Costs**—These are the incremental costs that would not be incurred if the contingency operation were not being carried out. Continuity of Operations **(COOP)**—The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander.

AFH 10-2502, USAF WEAPONS OF MASS DESTRUCTION (WMD) THREAT PLANNING AND RESPONSE HANDBOOK, 2001	The eight operational tasks of the WMD Threat Planning and Response Tree encompass the **three response phases**—pre-incident, **incident,** and post-incident—providing for enhanced planning and response for a terrorist WMD incident/attack. The Notification Operational Task. Notification begins when a report of the WMD incident/attack arrives at a link in the notification chain, whether it be the control tower, fire department, emergency room, security forces, or command post. All installation personnel should notify the proper authorities of a suspected terrorist incident. Typically, installations will use the primary and/or secondary crash nets to notify fire, medical, security forces, and the remainder of the DCG. This topic is discussed in greater detail in the section titled "The Notification and Resource Activation Process". NOTE: See the Notification and Resource Activation flow charts for a visual representation of the Notification Process in figures 17 and 18. 3. **Risk Assessment & Management:** Definition: Identify base shortfalls/vulnerabilities; identify the level of risk base commander is willing to accept. **Implement a Mission Recovery Plan** (Figure 19). This phase normally begins with an assessment of the area after the scene has been declared safe. The OSC has primary responsibility to approve all recovery operations. Restoration of the area is a long-range project, but general restoration steps should appear in the plan. **DRF**--Disaster Response Force; the organization used for disaster, accident, or **incident response**, command and control, and **recovery**.
AFMAN 10-2502, AIR FORCE INCIDENT MANAGEMENT SYSTEM (AFIMS) STANDARDS AND PROCEDURES, 2009	1.3.7.4. Department of Defense Directive (DODD) 3020.36, Assignment of National Security Emergency Preparedness (NSEP) Responsibilities to DOD Components. Each DOD component s**hall share the general responsibilities for emergency preparedness**, mobilization planning, and **crisis management in ensuring the continuity of government** in any national security or domestic emergency. 2.1.2. **Phases of Incident Management.** AFIMS phases of incident management include **prevention, preparation, response, recovery, and mitigation**. 3.3. For AFIMS, the **Comprehensive Emergency Management Plan (CEMP) 10-2** provides the comprehensive guidance, to include referencing other plans that are appropriate for the situation, for responding to an emergency incident that may affect an installation or its mission. 3.4. **Crisis Action Planning.** In a crisis, the time available for lengthy and detailed planning does not exist. Planners and operators are likely to be in a ―no plan‖ situation for contingencies not anticipated by deliberate planning. **They must develop courses of action, a CONOPS, and an IAP from scratch in a compressed timeframe. However, even though the crisis may not resemble existing operation plans in detail,** there are probably aspects of one or more plans in the database that could be adapted to the situation. Quality deliberate planning and mitigation efforts enhance the potential for success during crises. If the response to an incident has to be completely developed without adapting plans or parts of plans, the routine process of developing the CEMP10-2 in deliberate planning keeps the CAT, EOC, and response forces familiar with the procedures, policies, and installation response capabilities that assist with rapid development of IAPs. A2.4. **Incident Command Post (ICP).** According to NIMS and ICS, the ICP is the physical location at the tactical-level for on-scene incident command and management organization. Typically, it is comprised of the IC, Command Staff (Safety Officer, Liaison Officer, and Public Information Officer) and General Staff (Operations, Planning, Logistics, and Finance/Administration). Most Air Force incidents will not require the entire Command and General Staff. In most cases the tasks associated with the General Staff functions of Planning, Logistics, and Finance/Admin will be carried out by those in the EOC. It may also include other designated incident management officials and responders from Federal, State, local, and

	tribal agencies, as well as private sector, nongovernmental, and volunteer organizations. A2.8.3.1.1. Communications Unit. **A5.1. Incident Types**. Are used by the civilian authorities to categorize the incident. Incidents are categorized by five types based on complexity. Type 5 incidents are the least complex and Type 1 the most complex. A5.2. Table A5. 1. shows that incidents may be typed to make decisions about resource requirements.
AFMAN 10-2504, AIR FORCE INCIDENT MANAGEMENT GUIDANCE FOR MAJOR ACCIDENTS AND NATURAL DISASTERS, 2009	1.2. Mission. The missions of the **Air Force (AF) EM Program** are to save lives, minimize the **loss or degradation of resources, continuity of operations (COOP),** and sustain and restore operational capability in an ―all hazards‖ physical threat environment at AF installations worldwide. Major accident and natural disaster physical threats are defined in Chapter 2. 4.2. **Mission Continuation.** The installation commander may direct or prioritize mission-**essential activities to continue during major accident or natural disaster response and recovery operations** regardless of the threat posed. The importance of these missions should justify the increased risk to personnel and resources. The installation commander will use operational risk management tools to provide the decision-making basis upon which to allow critical missions to continue. Hazard areas must be identified. As a planned consequence, personnel will avoid those areas. In addition, this reduces the protective factor for others working in an uncontaminated area; personnel can initiate recovery actions to stabilize and continue the mission. 4.6. **Restoration.** The restoration, in concert with mission continuation tasks, officially begins when the IC advises the EOC Director that the incident has been sufficiently controlled or terminated and the security of the situation is sufficient to begin restoration activity. Consequently, the EOC directs and coordinates recovery inspections and reports damage by using ―quick looks‖ and detailed assessments. **Air Force Incident Management System (AFIMS)**—A methodology designed to incorporate the requirements of HSPD-5, the NIMS, the NRP, and OSD guidance while preserving the unique military requirements of the expeditionary Air Force. AFIMS provides the Air Force with an incident management system that is consistent with the single, comprehensive approach to incident management. **Continuity of Operations (COOP)**—The degree or state of being continuous in the conduct of functions, tasks or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander.
AFMAN 10-2507, READINESS AND EMERGENCY MANAGEMENT (R&EM) FLIGHT OPERATIONS, 2009	A2.3.2.9. **Estimate Operational Risk:** Based on reconnaissance and initial entry teams' assessments and CBRN detection grid results an operational risk assessment is given to the commander. The a**ssessment will be based on mission criticality and the risk to personnel.** EM personnel will consult with BEE on the health risks to personnel based on existing information prior to providing the commander an operational risk assessment on reducing individual protective equipment requirements or allowing personnel to re-enter the area or facility.

AFMAN 10-2602, NUCLEAR, BIOLOGICAL, CHEMICAL, AND CONVENTIONAL (NBCC) DEFENSE OPERATIONS AND STANDARDS, 2003	4.5. **Continuity of Operations.** Develop plans, checklists, and procedures to maintain **unit integrity and the continuity of operations for the WOC, SRC, and unit control centers.** Establish an alternate control center, or equivalent command and control function, with sufficient manning and redundant communications systems to maintain unit cohesion and mission continuity. **Alternate command and control elements and systems provide the ability to continue operations in the event of failure or damage to the primary element or system.** Update status boards and event logs to duplicate information available in the primary function. Locate the alternate function a reasonable distance from the primary to avoid damage or destruction of both functions from a single event. Consider using the alternate function as the off-shift beddown location for primary UCC personnel. 4.1.2. **Survival Recovery Center (SRC):** 4.1.2.1. The SRC gathers information, directs, and monitors execution of the installation NBCC defense survivability, recovery, and sustainment operations. The SRC collects, analyzes, prioritizes, displays, and reports information on the status of the base. It recommends courses of action and executes pre-planned and WOC-directed actions. The SRC objective is to concentrate resources and expertise at the right place and at the right time to implement the commander's direction.
AFI 10-2603, EMERGENCY HEALTH POWERS ON AIR FORCE INSTALLATIONS, 2005	1.5.2. **National Incident Management System (NIMS).** Established by HSPD-5, the NIMS provides a core set of concepts, principles, and terminology for incident command and multi-agency coordination of efforts responding to a domestic incident at all echelons of government (i.e., local, state, and federal). 1.5.3. **National Response Plan (NRP).** The NRP provides the national framework for domestic incident management across all categories of incident type. It establishes incident/potential incident monitoring and reporting protocols. It typically is enacted only for incidents of national significance, which include credible threats/indications/acts of terrorism within CONUS, major disasters or emergencies (as defined by the Stafford Act, Title 42, United States Code, Section 5121 et seq), catastrophic incidents, or unique situations that may require the Department of Homeland Security to aid in coordination of incident management.
AFMAN 10-2605, EDUCATION, TRAINING AND EXERCISE COMPETENCIES FOR COUNTER-CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR OPERATIONS, 2008	3.8.19. **Understand mission assurance/continuation planning considerations** and relationship to command, control, communications, computers and intelligence on Air Force installations 3.6.6. Use all available C-CBRN SMEs to **assess operational risk decision tools** against mission criticality [C-CBRN ETE COMPETENCIES, ASSOCIATED EDUCATION LEVELS OF LEARNING] **Consequence Management**— Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade or terrorist incidents. Also called CM. (JP 1-02) [CM activities serve to reduce the effects of a CBRN attack or event and assist in the restoration of essential operations and services at home and abroad in a permissive environment.] (AFDD 2-1.8) {Words in brackets apply only to the Air Force and are offered for clarity.}

AFI 10-2801, AIR FORCE CONCEPT OF OPERATIONS DEVELOPMENT, 2005	**Capabilities-Based Planning**—An approach where the focus is to identify a prioritized, integrated, and optimized set of air and space capabilities, including required support, that provide for specific effects. This set of effects-based capabilities is in turn tied to distinct, prioritized planning and programming actions that balance risk across the spectrum of military operations. **Capabilities Review and Risk Assessment**—The Air Force process for identifying and assessing the levels of capability needed to execute service-level concepts of operations, determining the status of these capabilities to achieve desired effects, and recommending courses of action to rectify overages, shortfalls, and gaps in the capability portfolio.

Appendix D: USAF Publications of Interest (Security/31 Series)

Publication Number	Text Extracts/Notes
AFI 31-201, SECURITY FORCES STANDARDS AND PROCEDURES, 2009	12.3.6. **Information**/Industrial Security **Incidents.** Summaries of major espionage cases, **independent research on insider threats**, and substantiated cases of industrial espionage/sabotage. 12.4.1. Provide the final report within 30 days of the conclusion of an exercise or operation or within 15 days after an incident via **Joint Lessons Learned Information System (JLLIS)**.
AFMAN 31-201V4, HIGH-RISK RESPONSE, 2002	2.5. **Phases of Response**. Generally, the actions taken to properly contend with accident, **disaster and incident scenes** consist of **notification, response**, response force actions, withdrawal, **recovery,** circulation and/or crowd control and release of information or permission for photography.
AFMAN 31-201V6, CIVIL DISTURBANCE, 2002	5.3.3. Vulnerability. Focuses on security weaknesses and high-risk targets (e.g., military installations, utility plants, dams or dike works). To assess the **vulnerability of the installation, consider**: **5.3.3.3. Communications availability/vulnerability.**
AFI 31-203, SECURITY FORCES MANAGEMENT INFORMATION SYSTEM (SFMIS), 2009	1.1.1. The **Security Forces Management Information System (SFMIS)** was developed primarily to meet the **Congressionally-mandated Defense Incident-Based Reporting System (DIBRS) requirements** and improve day-to-day operations of the Air Force Security Forces. It also provides statistical data for various users, and has grown to meet many other needs.
AFI 31-401, INFORMATION SECURITY PROGRAM MANAGEMENT, 2005	5.1.1. Everyone should be aware that advancing technology provides constantly changing means to quickly collect and transport information. The introduction of electronic storage or transmission devices into areas that store, process, and/or generate classified information increases the **risk to that information**. 9.3. **Information System (IS) Deviations.** Coordinate all security deviations involving information systems with the local ISPM and the supporting information assurance office to begin an evaluation on the **impact of the incident** to national security and the organization’s operations. If COMSEC material is involved, refer to AFI 33-212, Reporting COMSEC Deviations (will be incorporated in AFI 33-201, Volume 3, COMSEC User Requirements).
AFI 31-406, APPLYING NORTH ATLANTIC TREATY ORGANIZATION (NATO) PROTECTION STANDARDS, 2004	6.6.1. Military operations. Military commanders may authorize alternate procedures to meet mission requirements in accordance with DoD 5200.1-R, para 1-400; however, **mission impact** must be demonstrable. In doing so, consideration must be given to **risk management factors such as criticality, sensitivity, and value of the information;** analysis of the threats both known and anticipated; and vulnerability to exploitation.

Appendix E: USAF Publications of Interest (Civil Engineering/32 Series)

Publication Number	Text Extracts/Notes
AFMAN 32-1089, AIR FORCE MILITARY CONSTRUCTION AND FAMILY HOUSING ECONOMIC ANALYSIS GUIDE, 1996	**Risk**--The probability of an uncertain event occurring. 7. **Risk Assessment:** Identify the key variables which could possibly change to the extent that the recommendation would change.
AFI 32-2001, FIRE EMERGENCY SERVICES PROGRAM, 2008	6.1. **Risk Assessment and Management.** Fire Chiefs are responsible for managing available resources to minimize risk to people, property, and the environment. Risk decisions based on fact-based analysis provide a high degree of confidence that FES events will be managed appropriately with available resources. **Risk assessments based on actual emergency response data, tempered with sound professional judgment, provides the best opportunity for effectively managing FES events.** 6.1.1. Failure to provide adequate fire prevention services poses the greatest potential for long-term negative impact on fire safety. MAJCOM Directors, Installation Commanders and Fire Chiefs must ensure prevention programs including engineering controls, education, and enforcement receives the highest priority to effectively mitigate hazards. 6.1.2. The FES operations function is critical to the safety of people and property during emergencies. When emergencies occur, early intervention is the critical factor in reducing the potential for damage, injury and death. For this reason, response time standards are crucial to initial success. 6.1.3. The **level of service provided must be balanced based on risk**, probability of incidents and available resources. Although the RLS may provide resources needed to accomplish successful operations, **it must be measured against historic response data to ensure resources are sufficient for the risk.** When the CLS is reached, leaders must recognize the severe limitations of FES capability. There are, however, periods where the Installation Commander and Fire Chief must consider a reduction of service. 6.3. **Mitigating Risk.** Fire chiefs have wide latitude to manage risk by allocating resources according to local risk factors, to provide capability within the limits of available resources. 6.4. **Risk Management.** 6.4.1. The Fire Chief will establish management plans addressing reduced operational capability during periods of time when the department will operate below OLS as determined using the guide described in Attachment 4. The plan must include control measures implemented by the Fire Chief that describe both the p**robability and consequence of the potential risk**. These components include predicting the consequence of the identified risk and the probability of the event occurring. Control measures can include varying the available resources by time of day and day of the week based on the predicted probability while considering the consequence during both periods of risk. Attachment 4 - DETERMINING RISK PERIODS

AFPMAN 32-2004, AIRCRAFT FIRE PROTECTION FOR EXERCISES AND CONTINGENCY RESPONSE OPERATIONS, 2010	3. **Risk Management.** Fire fighting capability is dependent on two primary resources – fire fighting agent and personnel - discussed separately in paragraphs 4 and 5 below. An assumption that only one major fire incident will occur at the same time always exists. This document approaches risk management from a perspective of requiring the local risk managers to determine the acceptable levels of risk based on local risk factors. Generally, local risk factors include historic fire experience (if available), type and duration of the operation. 3.7. The **three elements of risk assessment are probability, severity, and exposure.** **Probability** involves using historical data to determine the likelihood an event will occur. **Severity** involves a subjective assessment of how severe the fire will be if it does occur. **Exposure** is a subjective assessment of the potential impact of the exposure (value of the material exposed and the time exposed) realizing that risk increases over time. Generally the probability of an ARFF fire is very low and the probability of a large fire is extremely low. Aside from crashes or explosions the severity of a fire is minimized by early intervention to prevent fire growth. Response time standards ensure early intervention by fire crews. Although fire safety standards make it unlikely a major fire will occur, local risk factors that can impact any of the three risk elements must also be factored in. For example, mission impact of even a small fire on a B-2 may have significantly more impact than a small fire on a C-130. **Risk Manager—**The technique or profession of assessing, minimizing, and preventing accidental loss to a business, as through the use of insurance, safety measures, etc.
AFHAN 32-2005, FIREFIGHTING GUIDE FOR CONTINGENCY OPERATIONS, 2009	4.2.4. **Communicate risk and capability issues** to the installation commander. For more information regarding reporting level of service capability see AFI 32-2001, chapter 6.5. 3.4. Operational Risk Management **(ORM)**. 3.4.1. Risk requires a subjective assessment of the probability that an FES emergency event will occur, and the expected severity of such an event. The probability factor relies heavily on **historic emergency response data** to predict future events. But for contingency operations, historical data is not available and assumptions must be made on which to estimate risk.
AFMAN 32-4004, EMERGENCY RESPONSE OPERATIONS, 1995	1.2. **Disaster Control Group (DCG).** The Air Force uses the installation DCG for initially responding to peacetime major accidents and natural disasters. It provides for on-scene command and control of military resources and functional expertise. 1.2.1. The DCG coordinates and directs operations and support requirements with the command post, unit control centers, specialized teams, and coordinates with civil and governmental authorities. 1.2.2. Primary and alternate functional representatives are required. Primary representatives should be organization commanders or chiefs; alternates should be functional experts delegated the same authority as the primary representative. 1.2.3. Composition and responsibilities vary with the resources, capabilities, and mission of each installation. Responding functional representatives perform duties inherent to their specific mission. If support requests exceed the capability of the installation, requests should be sent to higher headquarters. The following are recommended composition and response requirements for the DCG: 1.2.15. **Communications-Computers.** Advises the OSC on the capability and **availability of resources such as** cellular phones, secure radios, and secure telefacsimile. 3.1. General. **Actions taken for natural disaster response can be divided into four phases:** notification, initial emergency, sustained emergency, and recovery. In an actual response, these phases will most likely overlap. AFI 32-4001, Disaster Preparedness Planning and Operations contains policy on Air Force response to natural disasters. The following is a break-down of each phase and generic actions that could occur. Use Attachment 4 to develop checklists to support natural disaster response actions. **Disaster Support Group.**— A major command and field operating agency headquarters

	command and control element. It coordinates and supports the headquarters' response to a disaster. **Natural Disaster.**— All domestic emergencies except those created as a result of enemy attack or civil disturbance (Joint Publication 1-02). These may include hurricanes, tornadoes, storms, floods, high water, wind-driven water, tidal surge, tsunamis, earthquakes, volcanic eruptions, landslides, mud slides, severe snow storms, drought, or other catastrophe not caused by people.
AFI 32-7040, AIR QUALITY COMPLIANCE AND RESOURCE MANAGEMENT, 2007	2.11. Emergency Planning. Follow AFI 10-2501, Air Force Emergency Management (EM) Program Planning and Operations for **emergency planning and response to major accidents; natural disasters; terrorist use of weapons of mass destruction; and nuclear, biological, chemical and conventional warfare**. **Risk Management**—The process of evaluating alternative regulatory and nonregulatory responses to risk and selecting among them. The selection process requires consideration of impact to human health and the environment, legal, economic, military and social factors. **Risk Management Plan**—A plan that documents the actions a facility that stores, transports or uses regulated hazardous substances at levels exceeding established thresholds will take to prevent and mitigate their accidental release, and reduce the severity of releases that do occur. RMP requirements are found at 40 C.F.R. Part 68.
AFI 32-7064, INTEGRATED NATURAL RESOURCES MANAGEMENT, 2004	12.5.6. **Risk Assessment/Decision Analysis Processes.** Sound operational risk management will be the foundation of the Wildland Fire Management Plan. Identify the indices and/or fire danger rating system that will be used to assess wildfire risk and potential fire behavior. The indices and/or fire danger rating system must adequately describe fire hazard, severity, intensity, and other significant factors affecting the protection of life and property. Identify the environmental factors that will be measured prior to ignition of a prescribed fire treatment. Identify normal and unique weather patterns that affect fire behavior on the installation.

Appendix F: USAF Publications of Interest (Communications and Information/33 Series)

Publication Number	Text Extracts/Notes
AFPD 33-3, INFORMATION MANAGEMENT, 2006	Data Reliability—Refers to the accuracy and completeness of data, given the intended purposes for use. Data are reliable when they are (1) complete (they contain all the data elements (a unit of information with definable parameters (e.g., a Social Security number) and/or records required) and (2) accurate (they reflect the data entered at the source; or, if available, in the source documents). Air Force automated information processes enable data reliability by establishing/maintaining controls, that address **process risks**, to include, but not limited to, security, access, configuration controls and change management processes, system software, segregation of duties, **continuity of service**, authorization, completeness, accuracy, and confidentiality of data.
AFI 33-101, COMMANDERS GUIDANCE AND RESPONSIBILITIES, 2008	A2.2.5. Plan the evolution of systems supporting the installation users' missions; ensure war, support, and **contingency planning** are accomplished for communications and information requirements.
AFI 33-104, BASE LEVEL PLANNING AND IMPLEMENTATION, 2001	4.1.2. **Risk Analysis**--Identify, assess, and prioritize risks. A8.2.3. Another variable in project management is risk management. A project risk is a potential source of deviation from the project plan. These risks can have either a negative or positive outcome on the project. Negative risks are considered threats, while positive risks can be opportunities. **Risks—**Types of risk may include schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or systems, the number of simultaneous high risk projects to be monitored, funding availability, and program management risk. (OMB Circular No. A-130) **Risk Management**—1. Appropriate techniques should be applied to manage and mitigate risk during the acquisition of information technology. Techniques include, but are not limited to: prudent project management; use of modular contracting; thorough acquisition planning tied to budget planning by the program, finance and contracting offices; continuous collection and evaluation of risk-based assessment data; prototyping prior to implementation; post implementation reviews to determine actual project cost, benefits and returns; and focusing on risks and returns using quantifiable measures. (FAR 39) 2. Risk management is the process used by decision-makers to reduce or offset risk. The risk management process provides leaders and individuals a systematic mechanism to identify and choose the optimum course of action for any given situation. Risk management must become a fully integrated element of planning and executing an operation (See AFPD 90-9, Operational Risk Management; AFI 90-901, Operational Risk Management; and AFPAM 91-215, Operational Risk Management (ORM) Guidelines and Tools).

AFI 33-107V1, STRATEGIC AUTOMATED COMMAND CONTROL SYSTEM-DATA TRANSMISSION SUBSYTEM, 1997	CONTINGENCY INSTRUCTIONS: What to do if unable to support the Electronic Program Update at the scheduled time.
AFI 33-107V2, SACCS-DTS NETWORK SECURITY PROGRAM, 1997	2.4.3. Perform a risk analysis of the SACCS-DTS Network at 3 year intervals. Identify and document all assumptions and constraints associated with the network. Review and update the risk analysis on an annual basis or when major configuration changes are made. 2.4.5. **Direct a preliminary inquiry into each reported security incident involving the network.** Ascertain the extent of the incident, refer it to the appropriate agency for action, and assist in the investigation. Coordinate with the investigating agency to identify and implement necessary changes to prevent reoccurrence. 2.6.1.10. Establish security incident and reporting policy and procedures. 2.11.1. Network users must comply with the Network Security Plan and local security procedures. All users must immediately report security violations, incidents, or problems to their security officer. The applicable security officer will immediately relay the report up the chain of command to the NSM, and begin preliminary inquiry into the situation. AFSSM 5018, Risk Analysis Guide AFSSI 5021, Vulnerability and Incident Reporting
AFI 33-113, MANAGING AIR FORCE MESSAGING CENTERS, 2007	1.6.3. Establish an alternate site to ensure **continuity of operations** for their SIPRNET messaging equipment and services during times when the MMSC is offline.
AFI 33-115V1, NETWORK OPERATIONS (NETOPS), 2006	(SAF/XCI) 3.4.6. Be the lead for establishing an Air Force policy on **continuity of operations plans** for the AFNOSC, the NOSCs and NCCs. 3.8.2. Report to AFNOSCs and MAJCOM NOSCs all backdoors and unauthorized connections to Air Force networks discovered during the course of operations. Reports will be made immediately upon discovery if associated with an on-going incident and within 48 hours from discovery if not associated with an incident response action. 4.2.4.3. Draft SITREPs according to AFI 10-206, Operational Reporting. **Draft Operational Event/Incident Reports (OPREP3) according to AFI 10-206** to document and report significant network events affecting Defense Information Systems Network (DISN) connections not previously reported in SITREPs. 4.2.6.2. Provide real-time analysis, **response and reporting according to AFI 33-138** for network attacks and security incidents. Analyze customer impact of all network incidents, problems and alerts, and develop corrective actions or management changes. 4.5.4.11.45.20. Analyze customer impact, within the base, of all network incidents, problems and alerts, and develop corrective actions or management changes. 7.2.1.2. Operational Event/Incident Reports (OPREP3). OPREP3s are reported using operational channels, e.g., Command Posts, to notify commanders immediately of any event or incident that may attract international, national, US Air Force, or significant news media interest. They provide immediate up-channel notification of local network intrusions and probes, INFOCON level changes, and network degradations. They are generally tied to events. 7.2.1.5.1. TCNOs may be generated internally to direct the implementation of an **operational or a security vulnerability risk mitigation procedure** or fix action (e.g., software patch), or

	issued in response to DISA-generated Information Assurance Vulnerability Alerts (IAVA). TCNOs are used to address Air Force or theater wide incidents/problems and not for isolated internal incidents unless impact is determined to be system-wide.
AFI 33-129, WEB MANAGEMENT AND INTERNET USE, 2005	3.12.6. Ensuring certification and accreditation of their Web server before connecting to the network, as well as developing, coordinating, publishing, maintaining, and testing support plans for **contingency and service restoration**.
AFI 33-138, ENTERPRISE NETWORK OPERATIONS NOTIFICATION AND TRACKING, 2005	Enclave—Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest **mission assurance** category and security classification of the automated information system applications or outsourced information technology-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include LANs and the applications they host, backbone networks, and data processing centers. (AFI 33-202) 2.3.2. When delegated as the MAJCOM Designated Approving Authority (DAA), approve or disapprove applicable TCNO extension requests based on an assessment of the overall risk to the AFEN and to supported operations (see Section 3E). 2.10.2. Thoroughly understand the **risk to the AFEN and supported operational missions** before endorsing or approving TCNO extension requests. 3.16. Implementing Time Compliance Network Orders (TCNO). The goal of the TCNO process is the mitigation of risk to the AFEN through the implementation of network vulnerability countermeasures. 3.20.2. An extension does not grant the requesting agency the authority to accept the vulnerabilities or risks identified in the TCNO indefinitely; rather, it is approval to accept the risk for a specified period based on an operational risk management decision. 3.31.1.2. Conduct an o**perational risk management assessment of potential impact to local and Air Force missions** if vulnerable workstations are exploited. A4.1.9. Risk Mitigation Actions. Describe in detail what actions have been taken or processes put in place to mitigate the risk associated with the vulnerability. If some amount of the risk can be mitigated through other actions, this will help extension evaluation and approval officials assess the residual risk imposed on the AFEN and Air Force information systems if the extension is approved. A10.1. Vulnerability Reports (VR). Use the format below to submit initial, update, and final VR for **newly discovered vulnerabilities for which no risk mitigation procedure has been established.** If the newly discovered vulnerability was exploited or an incident actually occurred, go directly to Incident Reporting section (Section 5B). Prepare and submit a separate VR for each vulnerability being reported. Chapter 5— **INCIDENT AND VULNERABILITY REPORTING** Chapter 6— **SECURITY INCIDENT REPORTING** Chapter 7 — **SERVICE INTERRUPTION REPORTING**

AFI 33-200, INFORMATION ASSURANCE (IA) MANAGEMENT, 2008	**Mission Assurance Category**—Applicable to DoD ISs, the MAC reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. MACs are primarily used to determine the requirements for availability and integrity. DoD has three defined MACs (DoDD 8500.01): Mission Assurance **Category I**—Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a category I system is unacceptable and could include the immediate and sustained loss of mission effectiveness. Category I systems require the most stringent protection measures. [DoDD 8500.01] Mission Assurance **Category II**—Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Category II systems require additional safeguards beyond best practices to ensure adequate assurance. [DoDD 8500.01] Mission Assurance **Category III**—Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices. [DoDD 8500.01] **Specified Robustness**—The strength and level of confidence required of each IA solution is a function of the value of what is being protected (e.g., the mission assurance category or confidentiality level of the information being supported by the DoD IS) and the threat. 2.25.12.1. Report security violations and incidents to the DAA and Air Force network operations activities according to AFI 33-138, Enterprise Network Operations Notification and Tracking. 3.28. Incident Response and Reporting. AFI 33-138 defines reportable incidents, outlines SOPs for incident response, outlines user requirements, and establishes requirements for incident response in the AFNetOps hierarchy. Refer to AFNetOps instructions and procedures for classified message incidents.
AFI 33-210, AIR FORCE CERTIFICATION AND ACCREDITATION (C&A) PROGRAM (AFCAP), 2008	3.1.2.1. Mission Assurance Category (MAC I) systems (see DoDI 8500.2 for guidance). Air Force Network Operations (AFNETOPS)/CC or AFNETOPS/CV has connection approval authority. 3.1.2.2. MAC II systems. AFNETOPS/CC delegates connection approval authority to AFCA/CC or CV. 3.1.2.3. MAC III systems. AFNETOPS/CC delegates connection approval authority to AFCA/EV or EV Deputy. 2.6. Information System Owner. Must be a DoD official (O-6 or civilian equivalent), be a United States citizen, and have a level of authority commensurate with operating the IS on behalf of the Air Force so as to **manage the mission risk**.
AFI 33-360, PUBLICATIONS AND FORMS MANAGEMENT, 2006	1.2.2.2.2.2.4. Develops and maintains a contingency plan to ensure accessibility of publications and forms posted on the e-Publishing website when the site is down.

AFMAN 33-363, MANAGEMENT OF RECORDS, 2008	2.4.2. All **information** created in or received while carrying out the Air Force missions is categorized as a record. How long the record is needed to facilitate the work and the degree to which it must be controlled is an attribute of **its value to the mission or the agency, legal requirements, and its uniqueness.** 6.1.1.4.2.4. **Program managers** must identify vital records needed to **continue day-to-day operations without interruption or mission degradation after a disaster such as terrorist attack, hurricane, etc.** A5.2.3. Review of documentation created for the c**ontingency planning and risk assessment phase of emergency preparedness**. The offices performing those functions would be an obvious focus of an inventory.

Appendix G: USAF Publications of Interest (Special Management/90 Series)

Publication Number	Text Extracts/Notes
AFPD 90-8, ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH, 2004	1. This directive establishes the Air Force Environment, Safety, and Occupational Health (ESOH) program. This program identifies the ability of existing resources to meet operational requirements and assess risks caused by resource degradation or denial. 1.7. Make operational risk management a fundamental element at all levels of planning, decision-making, budgeting, acquisition, and all phases of operations in order to reduce the ESOH component of installation and weapon system total ownership costs.
AFPD 90-9, OPERATIONAL RISK MANAGEMENT, 2000	**Risk**—The probability and severity of loss or adverse impact from exposure to various hazards. **Risk Assessment**—The process of detecting hazards and their causes, and systematically assessing the associated risks. "Integrate ORM into Operations and Planning at all Levels" - To effectively apply risk management, commanders must dedicate time and resources to integrate risk management principles into the planning processes. **Risks are more easily assessed and managed in the planning stages of an operation.**
AFPD 90-13, MILITARY FLIGHT OPERATIONS QUALITY ASSURANCE, 2008	1.1. MFOQA is the analysis and trending of aircraft flight performance and system data to proactively enhance combat readiness through improvements in operations, maintenance, training, and safety functions. MFOQA provides tools for commanders to: establish a baseline for normal operations; identify, mitigate, and **monitor operational risks** while detecting precursors to aviation mishaps; and identify operational inefficiencies. MFOQA gives capabilities to multiple levels and functional areas to improve and enhance mission-effectiveness through awareness of abnormal trends, **continuous knowledge of aircraft systems performance**, and insight into the effectiveness of procedures, policy, and aircrew training on actual mission accomplishment.
AFPD 90-16, AIR FORCE STUDIES, ANALYSES, ASSESSMENTS, AND LESSONS LEARNED, 2008	**Risk**—The quantifiable level of exposure to an undesirable outcome based on consequence and likelihood. (AFI 10-604) 4.6. Operational Analyses. Analyses will sharpen the warfighters' edge by providing combat, operational, and support assessments, contingency and exercise support, risk assessments, and analysis of campaign and operational planning.
AFPD 90-17, ENERGY MANAGEMENT, 2009	Energy Security—Energy security includes physical security of infrastructure and supply, and **continuity of operations**. 3.9.4. Energy security shall be evaluated to determine potential short and long term energy disruptions and appropriate action shall be taken to mitigate energy security risks.

AFI 90-201,INSPECTOR GENERAL ACTIVITIES, 2009	A2.3.3.5.11. Evaluate the mediation plans for resolving Critical Infrastructure Program (CIP)-related problems affecting their mission assurance. 4.1.1. Scenarios. IG teams will attempt to create a realistic environment for evaluation while ensuring safety is not compromised. ORI **scenarios** evaluate garrison operations, contingency response (from both garrison and **continuity of operations (COOP) location**), and sustained performance. When possible, combine ORI scenarios with existing exercises, contingency events, or other MAJCOM scenarios. 4.5.5.1. Evaluate unit's ability to integrate deployed location procedures and requirements into unit's plans. Evaluate if the unit has a COOP plan which it exercises for contingency operations for incidents at the garrison location IAW **AFI 10-208, Continuity of Operations (COOP) Program**. Evaluate if all unit individuals know what actions to take during potential incidents. 4.7. **Ability To Survive and Operate (ATSO)**. Evaluate the unit's ability to conduct the full range of contingency operations, either in a stand alone, joint, or coalition forces operating environment, while simultaneously responding to or recovering from enemy attack, state/non-state use of CBRN weapons, major accidents, natural disasters, or HAZMAT incidents using the **Air Force Incident Management System (AFIMS).** 4.7.4.5. Evaluate ability to identify and mark CBRN hazard and hazard areas, conduct post-attack risk assessment, and implement management actions to reduce mission degradation.
AFI 90-801, ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH COUNCILS, 2005	1. Background. The Air Force will provide safe and healthful workplaces and conduct operations in a manner that minimizes risk to mission accomplishment while preserving resources, protecting the environment, and safeguarding Air Force personnel and the public both on and off the installation. 2.2. The ESOHC should ensure the appropriate level of ESOH assets are sustained, restored, and modernized to achieve the desired mission capability using a risk-based decision making process. 5.2.7. Champion inclusion of Air Force-unique ESOH needs in the Capabilities Review and Risk Assessment (CRRA) process and in the development of the Initial Capabilities Documents (ICDs), Capability Development Documents (CDDs), and Capability Production Documents (CPDs). 5.3.7. Use risk assessment methodology to identify and prioritize requirements that maximize mission performance and minimize ESOH risk and cost. **Risk**— A combination of the probability and severity of a loss or an adverse impact resulting from exposure to hazards. The greater the risk, the more likely it will cause a drain on resource capability and negatively affect the mission. ESOH - Environment, Safety, and Occupational Health

AFI 90-901, OPERATIONAL RISK MANAGEMENT, 2000	**ORM**—The systematic process of identifying hazards, assessing risk, analyzing risk control options and measures, making control decisions, implementing control decisions, accepting residual risks, and supervising/reviewing the activity for effectiveness. **Risk**—The probability and severity of loss or adverse impact from exposure to various hazards. **Risk Assessment**—The process of detecting hazards and their causes, and systematically assessing the associated risks. 3. ORM Principles. Four principles govern all actions associated with the management of risk. These principles, continuously employed, are applicable before, **during, and after all tasks and operations.** 3.1. Accept no unnecessary risk. Unnecessary risk comes without a commensurate return in terms of real benefits or available opportunities. All Air Force missions and daily routines involve risk. The most logical choices for accomplishing a mission are those that meet all mission requirements while exposing personnel and resources to the lowest acceptable risk. 3.2. Make risk decisions at the appropriate level. **Making risk decisions at the appropriate level establishes clear accountability.** Those accountable for the success or failure of the mission must be included in the risk decision process. 3.3. Accept risk when benefits outweigh the costs . All potential benefits should be compared to all potential costs. The process of weighing risks against opportunities and benefits helps to maximize unit capability. Even high risk endeavors may be undertaken when there is a well founded basis to believe that the sum of the benefits exceeds the sum of the costs. 3.4. Integrate ORM into operations and planning at all levels. To effectively apply risk management, **commanders must dedicate time and resources to integrate ORM principles into planning and operational processes.** Risk assessments of operations are most mission supportive when they are done as a normal way of conducting a mission, not an add-on process performed by people not otherwise involved. 4.5. Is a continuous, systematic decision-making tool consisting of six steps that define the process. The following is a description of the six-step process. 4.5.1. Identify the Hazards . Step one of the process involves application of appropriate hazard identification techniques in order to identify hazards associated with the operation or activity. **Hazard can be defined as any real or potential condition that can cause mission degradation.** 4.5.2. Assess the Risk . The assessment step involves the application of quantitative or qualitative measures to determine the probability and severity of ill effects potentially resulting from exposure to a hazard. 4.5.3. Analyze Risk Control Measures . Step three involves the evaluation of specific strategies and controls that reduce or eliminate risk. Effective mitigation measures reduce one of the three components (probability, severity or exposure) of risk. 4.5.4. Make Control Decisions . Decisions are made at the appropriate level and are based upon analysis of overall costs and benefits. Decision-makers choose the most mission supportive risk controls consistent with ORM principles. 4.5.5. Implement Risk Controls . Once control measures have been selected, an implementation strategy must be developed and carried out. 4.5.6. Supervise and Review. Risk management is a **process that continues throughout the life cycle of the system, mission, or activity.** Leaders at every level must fulfill their respective roles in ensuring controls are sustained over time. Once controls are in place, the process must be periodically reevaluated to ensure their effectiveness and mission supportiveness.

AFPAM90-902, OPERATIONAL RISK MANAGEMENT (ORM) GUIDELINES AND TOOLS, 2000	1. Introduction. **All US Air Force missions and our daily routines involve risk.** All operations, both on and off-duty, require decisions that include risk assessment as well as risk management. Each commander and supervisor, along with every individual, is responsible for identifying potential risks and adjusting or compensating appropriately. Risk decisions must be made at a level of responsibility that corresponds to the degree of risk, taking into consideration the significance of the mission and the timeliness of the required decision. Risk should be identified using the same disciplined, organized, and logical thought processes that govern all other aspects of military endeavors. **The USAF aim is to increase mission success while reducing the risk to personnel and resources to the lowest practical level in both on- and off-duty environments.** **Hazard**—Any real or potential condition that can cause mission degradation, injury, illness, death to personnel or damage to or loss of equipment or property. **Risk**—An expression of consequences in terms of the probability of an event occurring, the severity of the event and the exposure of personnel or resources to potential loss or harm. A general expression of risk as a function of probability, severity, and exposure can be written as: Risk = f(P, S, E). **Risk Assessment**—The process of detecting hazards and their causes, and systematically assessing the associated risks. Defines **Risk Management** in paras 1.1., 1.2, and 1.3. Six-Step Process of Operational Risk Management 11.1. The 5-M Model. The 5-M model, Figure 3., provides a basic framework for analyzing systems and determining the **relationships between composite elements that work together to perform the mission.** The 5-M's are Man, Machine, Media, Management, and Mission. Man, Machine, and Media interact to produce a successful Mission or, sometimes, an unsuccessful one. 11.3.3. Machine. Used as intended, limitations, interface with man. 11.3.3.1. Design: Engineering reliability and performance, ergonomics. 11.3.3.2. Maintenance: Availability of time, tools, and parts, ease of access. 11.3.3.3. Logistics: Supply, upkeep, repair. 11.3.3.4. **Tech data:** Clear, accurate, useable, available. A2.21. THE MISHAP/**INCIDENT INVESTIGATION.** Purpose, Method, Application, etc defined in this section.
AFI 90-1301, IMPLEMENTING MILITARY FLIGHT OPERATIONS QUALITY ASSURANCE , 2008	1.2. By **reducing aircrew risk, improving risk management, and enhancing situational awareness**, MFOQA effectively protects people, conserves aircraft, maximizes efficiency, and **improves readiness**. **2.2.6. Assess risk, identify mitigation measures, and monitor effectiveness.** 2.2.6.1. The appropriate reviewing body or commander evaluates risk exposure as measured by Military Flight Operations Quality Assurance (MFOQA) analysis results, initiates mitigation efforts when unacceptable levels of risk are identified, and monitors the effectiveness of the mitigation measures. 2.2.6.2. Mitigation measures include any means necessary, ranging from modification of procedures, aircraft limitations, or training syllabi, to simple aircrew, maintainer, or commander awareness efforts. 2.2.6.3. Groups or individuals implementing mitigation measures utilize further MFOQA analysis to monitor effectiveness and determine modifications or additional measures necessary, as required. 3.2.4. Conduct risk assessments on hardware or software using the Standard Practice for System Safety, MIL-STD-882D. The required formal risk acceptance must be in accordance with DoDI 5000.2, E.7.

AFI 90-1601, AIR FORCE LESSONS LEARNED PROGRAM, 2009	7.4.1. AF/A9L will coordinate with other HQ USAF directorates to ensure consideration of current actions addressing Air Force and Joint lessons implemented are incorporated into programmatic and risk assessment decision cycles. 4.2.2.1. Participative. The **lessons learned staff** performs two roles during the event. First, the lessons learned staff **participates in the unit's operational battle rhythm**, attending staff meetings, manning the Crisis Action Team, and/or **providing real-time inputs to the commander's planning and decision process.**
AFI 90-1701, ENERGY MANAGEMENT, 2009	11.2. Goals. 11.2.1. Identify Air Force assets and infrastructure dependencies critical to the execution of our missions, capabilities, and core functions. 11.2.2. Assess critical assets to determine vulnerabilities and risk of loss. 11.2.3. Prioritize critical assets to support management of risk and to apply scarce resources. Remediate risks through a risk management process. 11.2.4. Coordinate with existing programs for protection of critical assets in order to leverage existing processes where possible. 11.3.3. Field the Critical Asset Prioritization Methodology (CAPM) tool. This CAPM tool will allow prioritization of Air Force critical assets. This allows leadership to utilize its limited funding to remediate the most important critical assets at highest risk of being degraded or lost. 11.3.7. Build remediation recommendations that **provide Commanders with options to remediate their risk of loss of their critical assets** (for the critical supporting energy infrastructure, including new tactics, techniques, procedures, protection measures, implementation of redundancy capabilities, etc).

Appendix H: USAF Publications of Interest (Safety/91 Series)

Publication Number	Text Extracts/Notes
AFMAN 91-201, EXPLOSIVES SAFETY STANDARDS, 2008	Section 4A–Risk Assessments 4.1. **Requirements for Risk Assessments.** Risk assessments are required for all new or modified explosives, explosives operations, equipment and facilities. These risk assessments will be used to identify design and operations criteria (e.g., shielding, protective clothing). See Chapter 2 for reaction effect information to support risk assessments. Section 13C–Risk Management 13.6. **Risk Management.** Consistent with operational requirements, it is Air Force policy to manage risks associated with AE (see paragraph 1.1). Exceptions to this chapter's criteria are allowed only where equivalent protection is provided, or where risk assessment and risk management control is performed. **Risk**—The product of the probability or frequency that an accident will occur within a certain time and the accident's consequences to people, property or the environment. **Risk Assessment**—A method of determining and documenting hazards which may be present and controls for mitigating or eliminating those hazards.
AFI 91-202, THE US AIR FORCE MISHAP PREVENTION PROGRAM, 1998	9.6. **Risk Assessment and Management.** Accomplish an appropriate assessment/analysis of the safety and operational risks associated with all modification proposals and acquisition and development efforts. Program safety offices must ensure all necessary engineering and design data is produced and maintained to adequately document the risk decisions made, the design changes incorporated to reduce or eliminate hazards and any residual risks and hazards left in the system. Residual hazards and risk accepted and signed off by the appropriate authorities should be thoroughly documented and periodically reviewed by using and developing commands. This ensures that risk assessments are still appropriate and for available possible correction as part of a later modification or redesign. **Risk Assessment**— An evaluation of possible loss in terms of hazard or deficiency severity and mishap probability of occurrence. **Risk Assessment Code (RAC)**— An expression of the degree of risk in terms of hazard or deficiency severity and probability of occurrence. See AFI 91-301 for a discussion of RACs. **Risk Management**— The application of a systematic process or thinking to detect, assess, and control risk to enhance total organizational performance.

AFI 91-204, SAFETY INVESTIGATIONS AND REPORTS, 2008	DEPARTMENT OF DEFENSE HUMAN FACTORS ANALYSIS AND CLASSIFICATION SYSTEM (DOD HFACS) **Judgment and Decision-Making Errors** are factors in a mishap when behavior or actions of the individual proceed as intended yet the chosen plan proves inadequate to achieve the desired end-state and results in an unsafe situation. **AE201 Risk Assessment – During Operation** **Risk Assessment – During Operation** is a factor when the **individual fails to adequately evaluate the risks associated** with a particular course of action and this faulty evaluation leads to inappropriate decision and subsequent unsafe situation. This failure occurs in real-time when formal risk-assessment procedures are not possible. **Violations** are factors in a mishap when the actions of the operator represent willful disregard for rules and instructions and lead to an unsafe situation. Violations are deliberate. AV001 Violation - Based on Risk Assessment **Violation**- Based on Risk Assessment is a factor **when the consequences/risk of violating published procedures was recognized**, consciously assessed and honestly determined by the individual, crew or team to be the best course of action. Routine "work-arounds" and unofficial procedures that are accepted by the community as necessary for operations are also captured under this code. **Personnel Factors** are factors in a mishap if self imposed stressors or crew resource management affect practices, conditions or actions of individuals and result in human error or an unsafe situation. PP109 Mission Planning **Mission planning** is a factor when an individual, crew or team failed to complete all preparatory tasks associated with planning the mission, resulting in an unsafe situation. Planning tasks include information collection and analysis, coordinating activities within the crew or team and with appropriate external agencies, **contingency planning, and risk assessment.** **PP111 Task/Mission-In-Progress Re-Planning** **Task/**mission-in-progress re-planning is a factor when crew or team members fail to adequately reassess changes in their dynamic environment during mission execution and change their mission plan accordingly to **ensure adequate management of risk.** **Planned Inappropriate Operations** is a factor in a mishap when supervision fails to adequately assess the hazards associated with an operation and allows for unnecessary risk. It is also a factor when supervision allows non-proficient or inexperienced personnel to attempt missions beyond their capability or when crew or flight makeup is inappropriate for the task or mission. SP006 Risk Assessment – Formal **Risk Assessment** – Formal is a factor when supervision does not adequately evaluate the risks associated with a mission or when pre-mission risk assessment tools or risk assessment programs are inadequate.
AFPAM 91-211, USAF GUIDE TO AVIATION SAFETY INVESTIGATION, 2001	A8.2.2. Human Factors Definitions and Codes IB606 **RISK ASSESSMENT** is a factor when the individual fails to adequately evaluate potential risks associated with a selected course of action and this failure leads to an unsafe situation. IB905 **INVULNERABLE** is a factor when the individual demonstrates a "bullet proof" attitude that leads the individual to **ignore realistic threats or risks**.

AFPAM 91-216, USAF SAFETY DEPLOYMENT AND CONTINGENCY PAMPHLET, 2001	**Risk**—1. Probability and severity of loss linked to hazards. 2. See degree of risk. See also hazard; risk management. (JP 1-02) **Risk Assessment**—The identification and assessment of hazards (first two steps of risk management process). **Risk Management**—A process by which decision makers reduce or offset risk. Also called RM. See also risk. (JP 1-02)
AFI 91-217, SPACE SAFETY AND MISHAP PREVENTION PROGRAM, 2010	1.2.2. **Mission Assurance** and Space Safety. Space safety provides for **mission assurance by appropriately managing risks and increasing system availability**. Note: Space safety is only one aspect of mission assurance for space systems. There are other aspects of mission assurance that are beyond the scope of space safety and this document. 4.6.3. **Launch Operations Risk**. Independent risk budgets for a mission will be developed when the phases of flight meet the guidelines specified in the Range Commander's Council (RCC) Standard 321. Risk management responsibility directly corresponds with mission command and control responsibility/authority. **Launch and orbital risk management will apply quantitative risk analysis** consistent with DoD, RCC, AF and industry standards and practices. **Acceptable risk**—A predetermined criterion or standard for a maximum risk ceiling which permits the evaluation of cost, national priority interests, and number of tests to be conducted. **MISSION ASSURANCE**—An integrated engineering-level assessment of analysis, production, verification, validation, operation, maintenance, and problem resolution processes performed over the life cycle of a program by which an operator/user determines that there is an acceptable level of risk to employment of a system or end item to deliver an intended capability in an intended environment. The objective of the assurance process is to identify and mitigate design, production, test and operational deficiencies that could impact mission success. **MISSION FAILURE**—The inability of a space or ballistic system to complete its assigned mission. **MISSION RISK**—The risk that the mission will fail or be significantly degraded in capability. **Risk—See Collective risk.** A measure that takes into consideration both the probability of occurrence and the consequence of a hazard to a population or installation. Risk is measured in the same units as the consequence such as number of injuries, fatalities, or dollar loss. For Range Safety, risk is expressed as casualty expectation or shown in a risk profile.
AFMAN 91-223, AVIATION SAFETY INVESTIGATIONS AND REPORTS, 2004	7.2.1. Evaluating MOFE Recommendations. **OPRs are expected to use risk management principles during the evaluation**. For formal report recommendations, formal risk assessments are required. Risk assessments must consider the identified hazard and associated risk (as identified by the safety investigation and corrected as necessary by the OPRs and OCRs), the associated costs, benefits, schedule to implement, and residual risk assuming recommendation implementation. These assessments are then used for decision-making and at the MAJCOM level for the purpose of prioritizing open recommendations. Refer to AFI 90-901, Operational Risk Management, and AFPAM 90-902, Operational Risk Management (ORM) Guidelines and Tools, for information on appropriate risk management concepts, principles, and processes.

AFI 91-301, AIR FORCE OCCUPATIONAL AND ENVIRONMENTAL SAFETY, FIRE PROTECTION, AND HEALTH (AFOSH) PROGRAM, 1996	Section C—Hazard Abatement 16. **Risk Assessment Code (RAC)**. Evaluate each occupational hazard or deficiency and assign a RAC (Table 1.). Qualified safety, fire protection, and health personnel evaluate and assign RACs. Determine the mishap probability and severity for occupational safety and fire hazards and safety deficiencies according to the procedures in paragraphs 16.1. and 16.2. Determine the RAC by plotting the probability (A, B, C, or D) that a mishap will occur and the potential mishap severity (I, II, III, or IV) if it does happen. Attachment 7 provides procedures for determining RACs for health hazards or deficiencies. Attachment 8 provides procedures for determining RACs for fire deficiencies. Implementing interim control measures to reduce the level of risk associated with a particular hazard or deficiency will not affect the assigned RAC for corrective action purposes. **Risk Assessmen**t—A method of evaluating the occupational mishap potential, based upon severity and mishap probability associated with an identified occupational hazard or deficiency. **Risk Assessment Code (RAC)**—An expression of the degree of risk associated with an occupational hazard or deficiency that combines hazard severity and mishap probability into a single numeric identifier.

Appendix I: Coding Results – US Government Documents

			AFPD 10-2, 2006	AFPD 10-8, 2006	AFPD 10-24, 2006	AFI 10-204, 2010	AFI 10-208, 2005	AFI 10-211, 2008	AFPAM 10-219V2, 2008	AFPAM 10-219V3, 2008	AFPAM 10-219V8, 2007	AFH 10-222V3, 2008	AFH 10-222V14, 2008	AFH 10-222V16, 2005	AFI 10-245, 2009	AFI 10-246, 2004	AFMAN 10-401V2, 1998	AFI 10-802, 2002	AFI 10-2501, 2007	AFMAN 10-2502, 2009	AFMAN 10-2504, 2009	AFMAN 10-2602, 2003
OC No.	**Overall Category (OC)**	**Topic**	A3	A3	A3/5	A3	A3	A7C	A7S	A7C	A7C	A7C	A7C	A7C	A7S	SG	A3	A3	A7C	A7C	A7C	A7C
1	Mission	Mission Assurance	2	4	2	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	2
		Mission Assessment	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
		Mission to IT Dependencies	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1
2	Continuity Planning	Continuity Plan	1	2	2	1	3	4	4	3	1	3	1	1	2	2	1	1	3	2	3	3
		Preparedness	4	4	2	2	5	4	4	4	3	2	2	2	3	2	3	3	4	2	4	3
		Recovery	1	3	1	1	2	3	4	5	3	3	1	3	2	2	3	3	4	4	4	3
		Lessons Learned	1	2	2	2	2	2	2	3	2	3	3	1	4	1	2	1	3	2	3	3
		Scenario-Based Planning	1	2	2	3	2	3	3	3	2	1	1	1	2	2	2	1	3	2	2	3
		Organizational Resilience	1	2	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	2	2
		Critical Infrastructure Protection	1	2	4	1	2	1	3	1	1	2	1	1	3	2	1	2	2	1	3	1
3	Risk	Risk Management	2	2	2	1	3	1	2	1	1	3	3	1	4	4	1	1	2	3	3	2
		Risk Assessment	1	2	2	1	3	3	4	2	1	4	4	1	2	4	2	1	3	3	3	2
4	Incidents	Incident Response	1	2	1	1	1	1	1	4	1	1	1	1	3	1	1	1	3	4	5	2
		Incident Notification	1	1	1	1	1	3	2	2	1	4	1	1	1	1	1	3	3	3	4	2

			AFMAN 10-2605, 2008	AFMAN 31-201V4, 2002	AFI 32-2001, 2008	AFMAN 32-4004, 1995	AFI 32-7040, 2007	AFPD 33-3, 2006	AFI 33-101, 2008	AFI 33-115V1, 2006	AFI 33-138, 2005	AFI 33-200, 2008	AFMAN 33-363, 2008	AFI 90-201, 2009	AFI 90-901, 2000	AFI 90-1601, 2009	AFPAM 90-902, 2000	AFI 91-204, 2008	DoDD 3020.26, 2009	DoDD 3020.40, 2010
OC No.	**Overall Category (OC)**	**Topic**	A5	A7S	A7C	A7C	A7C	A6	A6	A6	A6	A6	A6	IG	SE	A9	SE	SE	USD(P)	USD(P)
1	Mission	Mission Assurance	2	1	1	1	1	2	1	1	2	3	1	1	1	1	2	1	1	3
		Mission Assessment	1	1	1	2	1	1	1	1	1	1	1	2	1	1	4	1	1	1
		Mission to IT Dependencies	2	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	2	1
2	Continuity Planning	Continuity Plan	1	2	2	2	2	1	1	2	1	1	2	2	1	1	1	1	2	1
		Preparedness	3	4	3	3	2	2	2	2	3	1	2	2	1	2	2	2	4	2
		Recovery	2	3	2	3	2	1	1	2	2	2	2	2	1	1	1	1	2	2
		Lessons Learned	2	3	1	2	2	1	1	2	3	2	1	2	2	5	2	2	1	2
		Scenario-Based Planning	2	2	1	2	1	1	1	2	2	1	1	3	1	1	5	2	1	1
		Organizational Resilience	1	1	1	1	1	1	1	2	2	1	1	1	1	1	2	3	1	1
		Critical Infrastructure Protection	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	3
3	Risk	Risk Management	2	1	3	1	3	1	1	2	2	2	1	2	4	1	5	2	2	4
		Risk Assessment	2	1	3	1	2	1	1	1	2	2	2	2	4	2	5	3	1	3
4	Incidents	Incident Response	1	4	3	3	1	2	1	2	3	2	1	1	1	1	1	1	1	1
		Incident Notification	1	3	3	3	1	1	1	2	4	2	1	1	1	1	1	1	1	1

			DoDI 3020.42, 2006	DoDI 3020.45, 2008	DoDD 8500.01E, 2002	DoDI 8500.2, 2003	NIST SP 800-27 Rev. A, 2004	NIST SP 800-30, 2002	NIST SP 800-34 Rev. 1, 2009	NIST SP 800-37 Rev. 1, 2010	NIST SP 800-39 Rev. 2, 2008	NIST SP 800-55 Rev. 1, 2008	NIST SP 800-60 V1, Rev.1, 2008	NIST SP 800-60 V2, Rev.1, 2008	NIST SP 800-61 Rev. 1, 2008
OC No.	**Overall Category (OC)**	**Topic**	USD(P)	USD(P)	CIO	C3I	NIST	NIST	NIST	NIST	NIST	NIST	NIST	NIST	NIST
1	Mission	Mission Assurance	1	3	3	4	1	1	1	2	2	2	1	1	1
		Mission Assessment	1	1	1	1	1	1	1	1	1	1	1	1	1
		Mission to IT Dependencies	3	1	3	1	1	2	2	2	3	4	1	1	1
2	Continuity Planning	Continuity Plan	4	1	1	3	3	2	5	2	1	2	1	2	4
		Preparedness	4	2	2	3	3	2	4	2	2	2	3	3	3
		Recovery	2	3	3	3	3	3	5	3	2	2	3	3	4
		Lessons Learned	1	2	2	2	3	3	3	3	3	3	4	3	4
		Scenario-Based Planning	1	1	1	1	2	2	3	1	1	1	2	2	4
		Organizational Resilience	1	3	1	1	1	1	3	2	3	1	1	1	1
		Critical Infrastructure Protection	2	4	1	1	2	1	3	1	2	1	3	2	2
3	Risk	Risk Management	1	4	1	2	3	4	3	5	4	2	3	3	1
		Risk Assessment	2	4	2	3	4	5	3	3	3	3	1	2	3
4	Incidents	Incident Response	1	2	2	3	1	2	3	2	2	3	1	1	5
		Incident Notification	1	1	1	1	1	1	4	1	2	1	1	2	4

Appendix J: Coding Results – Non-US Government Documents

			ITGI COBIT 4.1, 2007	OCTAVE V2.0 (CMU), 2001	ISO/IEC 27000, 2009	ISO/IEC 27001, 2005	ISO/IEC 27002, 2005	ISO/IEC 27003, 2010	ISO/IEC 27004, 2009	ISO/IEC 27005, 2008	ITIL - Service Support V2, 2000	ITIL - Service Delivery V2, 2001
OC No.	**Overall Category (OC)**	**Topic**	ITGI	CMU	ISO	ISO	ISO	ISO	ISO	ISO	OGC	OGC
1	Mission	Mission Assurance	3	1	2	1	1	1	1	2	1	1
		Mission Assessment	4	1	1	1	1	1	1	1	1	1
		Mission to IT Dependencies	4	2	1	1	1	1	1	3	1	2
2	Continuity Planning	Continuity Plan	4	1	1	2	4	1	1	2	2	4
		Preparedness	5	3	2	3	4	2	2	2	3	5
		Recovery	3	2	1	2	3	2	1	1	2	4
		Lessons Learned	2	2	2	2	3	1	1	3	1	3
		Scenario-Based Planning	2	2	1	1	2	2	1	4	1	3
		Organizational Resilience	2	3	1	1	1	1	1	1	1	1
		Critical Infrastructure Protection	4	4	1	1	2	1	1	1	1	1
3	Risk	Risk Management	4	4	3	3	3	2	2	4	1	4
		Risk Assessment	4	3	3	4	4	3	2	4	1	4
4	Incidents	Incident Response	4	2	1	1	2	1	1	2	3	3
		Incident Notification	3	2	1	2	3	2	2	1	3	3

Bibliography

Abrams, M., Jajodia, S., & Podell, H. (Eds.). (1995). *Information Security: An Integrated Collection of Essays*. Los Alamitos, CA: IEEE Computer Society Press.

AF/A3O. "Building Air Force Core Unit Mission Essential Task Lists (METLs)." Electronic Staff Summary Sheet. A3O-AOBR, 7 March 2008.

Air Force Safety Center. (2005). *Risk Management Information System (RMIS) User's Guide*. Kirtland AFB, NM: Air Force Safety Center, August 2005. Retrieved from https://rmis.kirtland.af.mil/downloads/RMIS_Users_Guide.pdf

Air Force Space Command. (2009). *The United States Air Force Blueprint for Cyberspace*. Peterson AFB, CO: HQ AFSPC, 2 November 2009.

Air Force e-Publishing. (n.d.). *Obsolete Publications*. Retrieved from http://www.e-publishing.af.mil/obsoleteproducts/

Alberts, C.J. & Dorofee, A.J. (2001). *OCTAVE^{SM} Criteria, Version 2.0*. Technical Report CMU/SEI-2001-TR-016. Pittsburgh, PA: Carnegie Mellon University.

Alberts, C.J. & Dorofee, A.J. (2005). *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments*. Carnegie Mellon University Networked Systems Survivability Program Report CMU/SEI-2005-TN-032.

Alberts, C. J., Dorofee, A.J., Stevens, J., & Wooky, C. (2003). *Introduction to the OCTAVE approach*. Pittsburgh, PA: Carnegie Mellon University. Retrieved from www.cert.org/octave/approach_intro.pdf

Alberts, D.S. (2002). *Information age transformation: getting to a 21st century military*. CCRP Publication Series, Command and Control Research Program (CCRP), US Office of the Assistant Secretary of Defense. Retrieved from http://www.dodccrp.org/files/Alberts_IAT.pdf

Alberts, D.S., Garstka, J.J, & Stein, F.P. (1999). *Network centric warfare : developing and leveraging information superiority*. CCRP Publication Series, DoD C4ISR Cooperative Research Program, US Office of the Assistant Secretary of Defense. Retrieved from http://www.dodccrp.org/files/Alberts_NCW.pdf

Alberts, D.S. & Hayes, R.E. (2006). *Understanding command and control*. CCRP Publication Series, Command and Control Research Program (CCRP), US Office of the Assistant Secretary of Defense. Retrieved from http://www.dodccrp.org/files/Alberts_UC2.pdf

Anderson, E., Choobineh, J., & Grimaila, M.R. "An Enterprise Level Security Requirements Specification Model," *Proceedings of the 38th Annual Hawaii International Conference (HICSS 2005).* 186-196, January 2005.

Avitia, Serafin V. *Developing Network Situational Awareness Through Visualization of Fused Intrusion Detection System Alerts.* MS thesis, AFIT/GCS/ENG/08-23. School of Electrical and Computer Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, June 2008.

Baker, S., Waterman, S., & Ivanov, G. *In the Crossfire: Critical Infrastructure in the Age of Cyber War.* Santa Clara, CA: McAfee, 2009.

Berelson, B. (1952). *Content Analysis in Communication Research.* New York, NY: New York Free Press.

Bickford, M., Kreitz, C., van Renesse, R., Constable, R. "An Experiment in Formal Design using Meta-Properties," *Proceedings of DARPA Information Survivability Conference & Exposition II, Vol. 2,* 100-107, 2001.

Carroll, Sean C.M. *Mission Impact Analysis Visualization for Enhanced Situational Awareness.* MS thesis, AFIT/GCO/ENG/08-01. School of Electrical and Computer Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2008.

Cerullo, V. & Cerullo, M.J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management, 21*(3), 70-78.

Chase, Lee E. *Integration of Cyber Situational Awareness Into System Design and Development.* MS thesis, AFIT/ISE/ENV/09-J02. School of Systems and Engineering Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, June 2009.

CNCI. (2010). *The Comprehensive National Cybersecurity Initiative.* Washington: Executive Office of the President of the United States of America, 3 March 2010. Retrieved from http://www.whitehouse.gov/sites/default/files/Cybersecurity.pdf

COBIT v4.1. (2007). *Control Objectives for Information and related Technology.* IT Governance Institute. Retrieved from http://www.isaca.org/cobit

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement, 20,* 37-46.

COSO. (2004). *Enterprise Risk Management — Integrated Framework.* Committee of Sponsoring Organizations of the Treadway Commission (COSO). Retrieved from http://www.coso.org

CSU. (2010). *An Introduction to Content Analysis.* Colorado State University, CO. Retrieved on November 6, 2009, from http://writing.colostate.edu/guides/research/content/pop2a.cfm

D'Amico, A. & Salas, S. "Visualization as an Aid for Assessing the Mission Impact of Information Security Breaches," *Proceedings of DARPA Information Survivability Conference and Exposition, Vol. 2*, 18-24, 2003.

Daniel, L. (2010, May 10). Officials warn of 'phishing' scams targeting troops. *USAF News.* Retrieved from http://www.af.mil/news/story.asp?storyID=123203895

Davenport, T.H. & Prusak, L. (2000). *Working Knowledge: How Organizations Manage What They Know*. Boston, MA: Harvard Business School Press.

Denning, D. (1999). *Information Warfare and Security.* Upper Saddle River, NJ: Pearson Education, Inc.

Denzin, N. K., & Lincoln, Y. S. (2000). *Handbook of Qualitative Research.* Thousand Oaks, CA: Sage Publications.

Department of Defense. (2001). *Department of Defense Dictionary of Military and Associated Terms.* JP 1-02. Washington: United States Department of Defense, Joint Chiefs of Staff, 12 April 2001 (As Amended Through 31 October 2009).

Department of Defense. (2002a). *Functions of the Department of Defense and Its Major Components.* DoDD 5100.01. Washington: United States Department of Defense, 1 August 2002.

Department of Defense. (2002b). *Information Assurance (IA).* DoDD 8500.01E. Washington: United States Department of Defense, 24 October 2002.

Department of Defense. (2002c). *Universal Joint Task List (UJTL).* CJCSM 3500.04C. Washington: United States Department of Defense, 1 July 2002.

Department of Defense. (2003). *Information Assurance (IA) Implementation.* DoDI 8500.2. Washington: United States Department of Defense, 6 February 2003.

Department of Defense. (2006a). *Defense Continuity Plan Development.* DoDI 3020.42. Washington: United States Department of Defense, 17 February 2006.

Department of Defense. (2006b). *Information Operations*. JP 3-13. Washington: United States Department of Defense, Joint Chiefs of Staff, 13 February 2006.

Department of Defense. (2006c). *Joint Operation Planning*. JP 5-0. Washington: United States Department of Defense, Joint Chiefs of Staff, 25 December 2006.

Department of Defense. (2007). *DoD Information Assurance Certification and Accreditation Process (DIACAP)*. DoDI 8510.01. Washington: United States Department of Defense, Joint Chiefs of Staff, 28 November 2007.

Department of Defense. (2008). *Defense Critical Infrastructure Program (DCIP) Management.* DoDI 3020.45. Washington: United States Department of Defense, 21 April 2008.

Department of Defense. (2009a). *Department of Defense Continuity Programs.* DoDD 3020.26. Washington: United States Department of Defense, 9 January 2009.

Department of Defense. (2009b). *DoD Architecture Framework - Version 2.0: Volume 1: Introduction, Overview, and Concepts Manager's Guide.* DoDAFV2, Vol 1. Washington: United States Department of Defense, Assistant Secretary of Defense for Networks and Information Integration and Department of Defense Chief Information Officer, 28 May 2009.

Department of Defense. (2010). *DoD Policy and Responsibilities for Critical Infrastructure.* DoDD 3020.40. Washington: United States Department of Defense, 14 January 2010.

Department of Defense. (n.d.). *The DoD Issuance Numbering System.* Washington, DC: DoD. Retrieved on 22 March 2010 from http://www.dtic.mil/whs/directives/corres/writing/Issuance_Numbering.doc

Department of Defense Inspector General. *Contingency Planning for DoD Mission-Critical Information Systems*. Report No. D-2008-047. Washington: ODIG, 2008.

Department of Homeland Security (2008). *National Response Framework.* Washington, DC: Department of Homeland Security. Retrieved from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

Department of the Air Force. (2000a). *Operational Risk Management.* AFI 90-901. Washington: HQ USAF, 1 April 2000.

Department of the Air Force. (2000b). *Operational Risk Management (ORM) Guidelines and Tools.* AFPAM 90-902. Washington: HQ USAF, 14 December 2000.

Department of the Air Force. (2003). *Format and Content of Mission Directives.* AFI 10-101. Washington: HQ USAF, 12 February 2003.

Department of the Air Force. (2005a). *Continuity of Operations (COOP) Program.* AFI 10-208. Washington: HQ USAF, 1 December 2005.

Department of the Air Force. (2005b). *Enterprise Network Operations Notification and Tracking.* AFI 33-138. Washington: HQ USAF, 28 November 2005.

Department of the Air Force. (2006a). *Air Force Critical Infrastructure Program (CIP).* AFPD 10-24. Washington: HQ USAF, 28 April 2006.

Department of the Air Force. (2006b). *Homeland Defense and Civil Support.* AFPD 10-8. Washington: HQ USAF, 7 September 2006.

Department of the Air Force. (2006c). *Network Operations (NETOPS).* AFI 33-115V1. Washington: HQ USAF, 24 May 2006.

Department of the Air Force. (2006d). *Publications and Forms Management.* AFI 33-360. Washington: HQ USAF, 18 May 2006.

Department of the Air Force. (2007). *Air Force Emergency Management (EM) Program Planning and Operations.* AFI 10-2501. Washington: HQ USAF, 24 January 2007.

Department of the Air Force. (2008a). *Air Force Lessons Learned Program.* AFI 90-1601. Washington: HQ USAF, 26 June 2008.

Department of the Air Force. (2008b). *Civil Engineer Disaster and Attack Preparations.* AFPAM 10-219V2. Washington: HQ USAF, 9 June 2008.

Department of the Air Force. (2008c). *Civil Engineer Disaster and Attack Recovery Procedures.* AFPAM 10-219V3. Washington: HQ USAF, 9 June 2008.

Department of the Air Force. (2008d). *Education, Training and Exercise Competencies for Counter-Chemical, Biological, Radiological and Nuclear Operations.* AFMAN 10-2605. Washington: HQ USAF, 30 June 2008.

Department of the Air Force. (2008e). *Management of Records.* AFMAN 33-363. Washington: HQ USAF, 1 March 2008.

Department of the Air Force. (2008f). *Safety Investigation and Reports.* AFI 90-204. Washington: HQ USAF, 24 September 2008.

Department of the Air Force. (2009a). *Air Force Incident Management Guidance for Major Accidents and Natural Disasters*. AFMAN 10-2504. Washington: HQ USAF, 1 December 2009.

Department of the Air Force. (2009b). *Air Force Incident Management System (AFIMS) Standards and Procedures*. AFMAN 10-2502. Washington: HQ USAF, 25 September 2009.

Department of the Air Force. (2009c). *Inspector General Activities.* AFI 90-201. Washington: HQ USAF, 17 June 2009.

Department of the Air Force. (2010). *Cyberspace Operations (Topline Coordination Draft v4).* AFDD 3-12. . Washington: HQ USAF, March 2010.

Department of the Air Force Civil Engineer. *USAF Emergency Program Management Senior Leader Primer.* Washington, DC: HQ USAF, 2006.

Donley, M. B. (1995). Problems of Defense Organization and Management. *Joint Forces Quarterly (JFQ), Summer 1995,* 86-94.

Executive Order No. 13010. (1996). *Critical Infrastructure Protection.* Federal Register; 61 FR 37347, 15 July 1996. Retrieved from http://www.archives.gov/federal-register/executive-orders/1996.html

Fortson, Larry W. *Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology.* MS thesis, AFIT/GIR/ENV/07-M9. School of Systems and Engineering Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2007.

Fortson, L. W. & Grimaila, M. R. "Development of a Defensive Cyber Damage Assessment Framework," *Proceedings of the 2007 International Conference on Information Warfare and Security (ICIW 2007).* Monterey, CA: Naval Postgraduate School, 2007.

GAO. (1996). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* Chapter Report. Washington: United States General Accounting Office.

Gerber, M. & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16-30. doi:10.1016/j.cose.2004.11.002

Goldman, R.P., Heimerdinger, W., Harp, S.A., Geib, C.W., Thomas, V., & Carter, R.L. "Information modeling for intrusion report aggregation," *Proceedings of DARPA Information Survivability Conference & Exposition II, 2001 (DISCEX '01), Vol. 1,* 329-342, 2001.

Grimaila, M. R. & L. W. Fortson. "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process," *Proceedings of the 2007 IEEE Computational Intelligence for Security and Defense Applications (CISDA 2007).* 206-212. Honolulu, HI, 2007.

Grimaila, M.R., Fortson, L.W., & Sutton, J.L. "Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process," *Proceedings of the 2009*

International Conference on Security and Management (SAM09), Las Vegas, NV, 2009.

Goodall, J.R., D'Amico, A.D., & Kopylec, J. "Camus: Automatically Mapping Cyber Assets to Missions and Users," *2009 IEEE Military Communications Conference.* Boston MA, October 2009.

Hellesen, Denzil L. *An Analysis of Information Asset Valuation (IAV) Quantification Methodology for Application with Cyber Information Mission Impact Assessment (CIMIA).* MS thesis, AFIT/GIR/ENV/08-M11. School of Systems and Engineering Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2008.

Homeland Security. (2008). *Homeland Security Presidential Directive 20: National Continuity Policy*. Retrieved from http://www.dhs.gov/xabout/laws/gc_1219245380392.shtm

IATRP. (2003). INFOSEC Assurance Capability Maturity Model (IA-CMM) Version 3.0. *INFOSEC Assessment Training and Rating Program (IATRP).* Retrieved from http://www.iatrp.com/iacmm.cfm

IEC/ISO. (2009). *Risk management – Risk assessment techniques.* ISO 31010. Geneva, Switzerland.

(ISC)^2. (2009). Common Body of Knowledge (CBK). *International Information System Security Certification Consortium, Inc.* Retrieved from http://www.isc2.org/cgi-bin/content.cgi?category=8

ISO. (2009a). *Risk management — Principles and guidelines.* ISO 31000. Geneva, Switzerland.

ISO. (2009b). *Risk management — Vocabulary*. ISO Guide 73. Geneva, Switzerland.

ISO. (2010). About ISO. *International Organization for Standardization.* Retrieved from http://www.iso.org/iso/about.htm

ISO/IEC. (2005). *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC 27001. Geneva, Switzerland.

ISO/IEC. (2008). *Information technology — Security techniques — Information security risk management*. ISO/IEC 27005. Geneva, Switzerland.

ISO/IEC. (2009). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. ISO/IEC 27000. Geneva, Switzerland.

ISSA. (2005*).* Generally Accepted Information Security PrinciplesV3.0 (GAISP). *Information Systems Security Association (ISSA).* Retrieved from http://www.issa.org/gaisp/_pdfs/v30.pdf

I^{2}SF. (2005). Generally Accepted System Security Principles (GASSP). *International Information Security Foundation (I^{2}SF).* Retrieved from http://web.mit.edu/security/www/gassp2.html

ITGI. (2010). About ITGI. *IT Governance Institute.* Retrieved from http://www.itgi.org/

Jajodia, S., Ammann, P., and McCollum, C.D. (1999). Surviving Information Warfare Attacks. *IEEE Computer, 32*(4), 57-63.

Jos, B. & Culbertson, T. "Leveraging Net-Centric Monitoring Techniques with Information Fusion to Increase US Air Force Information Dominance," *Military Communications Conference (MILCOM 2006),* 1-6, Washington, DC, 2006

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Landis, J.R., & Koch, G.G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*, 159- 174.

Lowry, R. (2010). Kappa as a Measure of Concordance in Categorical Sorting [On-line Software]. Available from http://faculty.vassar.edu/lowry/kappa.html

Lyle, A. (2009, November 20). Air Force leaders speak at 2009 Global Warfare Symposium. *USAF News.* Retrieved from http://www.af.mil/news/story.asp?storyID=123178818

Melliar-Smith, P.M., Moser, L.E., Kalogeraki, V., Narasimhan, P. "Realize: Resource Management for Soft Real-Time Distributed Systems," *Proceedings of DARPA Information Survivability Conference and Exposition, 2000 (DISCEX '00), Vol. 1,* 281-293, 2000.

Millette, C. D. (2010, March 17). Air Force officials to implement hand-held device changes. *USAF News.* Retrieved from http://www.af.mil/news/story.asp?storyID=123195331

Moore, R.A., Kewley, D.L., Parks, R.C., Tinnel, L.S. "The Information Battlespace preparation experiment," *Proceedings of DARPA Information Survivability Conference & Exposition II, 2001 (DISCEX '01), Vol. 1,* 352-366. 2001.

Moss, M. & Townsend, A. in Digital Infrastructures: Enabling Civil and Environmental Systems Through Information Technology, R. Zimmerman, T. Horan (Eds.) (Routledge, London, 2004), 141–152.

National Institute of Standards and Technology. (2002). *Risk Management Guide for Information Technology Systems.* NIST Special Publication 800-30. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, March 2008.

National Institute of Standards and Technology. (2004a). *Engineering Principles for Information Technology, Security (A Baseline for Achieving Security), Revision A.* NIST Special Publication 800-27, Revision A. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, June 2004.

National Institute of Standards and Technology. (2004b). *Standards for Security Categorization of Federal Information and Information Systems*. FIPS Publication 199. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, February 2004.

National Institute of Standards and Technology. (2008a). *Computer Security Incident Handling Guide.* NIST Special Publication 800-61, Revision 1. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, March 2008.

National Institute of Standards and Technology. (2008b). *Performance Measurement Guide for Information Security.* NIST Special Publication 800-55, Revision 1. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, July 2008.

National Institute of Standards and Technology. (2008c). *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories.* NIST Special Publication 800-60V1, Revision 1. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, August 2008.

National Institute of Standards and Technology. (2009). *Contingency Planning Guide for Federal Information Systems (Draft).* NIST Special Publication 800-34, Revision 1. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, October 2009.

National Institute of Standards and Technology. (2010a). *Guide for Applying the Risk Management Framework to Federal Information Systems.* NIST Special Publication 800-37, Revision 1. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce, February 2010.

National Institute of Standards and Technology. (2010b). Special Publications (800 Series). Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

Office of Government Commerce. (2000). Service Support. *IT Infrastructure Library.* Norwich, United Kingdom: The Stationery Office.

Office of Government Commerce. (2001). Service Delivery. *IT Infrastructure Library.* Norwich, United Kingdom: The Stationery Office.

OCTAVE. (2004). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). *CERT Coordination Center, Software Engineering Institute.* Carnegie Mellon University. Retrieved from http://www.cert.org/octave

Parker, D.B. (2007). Comparison of Risk-Based and Diligence-Based Idealized Security Reviews. *EDPACS, Sep/Oct 2007, 36*(3/4), 1-12.

Petrocelli, T.D. (2005). *Data Protection and Information Lifecycle Management.* Upper Saddle River, New Jersey: Pearson Education, Inc.

Pipkin, D.L. (2000). *Information Security Protecting the Global Enterprise.* Hewlett-Packard Company.

Quadrennial Defense Review. (2010). "Quadrennial Defense Review Report," United States Department of Defense, February 2010.

Roberts, C. M. (2004). *The Dissertation Journey: A Practical and Comprehensive Guide to Planning, Writing, and Defending Your Dissertation.* Thousand Oaks, CA: Corwin Press.

Rosenzweig, P. (2009). *National Security Threats in Cyberspace – Post Workshop Report.* Retrieved from http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf

Rubin, H.A. (2010). Return on IT: The Holy Grail of the Business Value of IT. *Wall Street and Technology*, *28*(2), 15.

Secretary of Defense. *Defense Readiness Reporting System – Primer for Senior Leaders.* Washington: Office of the Secretary of Defense, OUSD Personnel and Readiness, 3 March 2006.

Shaw, Alfred K. *A Model for Performing Mission Impact Analysis of Network Outages*. MS thesis, AFIT/GCS/ENG/07-10. School of Electrical and Computer Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2007.

Singer, P. W. (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. Penguin Press; New York, NY.

Stanley, Jeffrey E. *Enabling Network Centric Warfare Through Operational Impact Analysis Automation.* MS thesis, AFIT/GIA/ENG/05-05. School of Electrical and Computer Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2005.

Stanley, J.E., Mills, R.F., Raines, R.A., & Baldwin, R.O. "Correlating Network Services with Operational Mission Impact," *Military Communications Conference (MILCOM 2005)*,1-7, Atlantic City, New Jersey, Oct 2005.

Strijbos, J., Martens, R., Prins, F., & Jochems, W. (2006). Content analysis: What are they talking about? *Computers & Education*, *46*, 29-48. doi: 10.1016/j.compedu.2005.04.002

Stemler, S. (2001). An overview of content analysis. *Practical Assessment, Research & Evaluation*, *7*(17). Retrieved March 9, 2010 from http://PAREonline.net/getvn.asp?v=7&n=17

Soo Hoo, K. J. (2000). *How Much Is Enough? A Risk-Management Approach to Computer Security* (Working Paper). Palo Alto, CA: Consortium for Research on Information Security and Policy (CRISP). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.4127&rep=rep1&type=pdf

Sorrels, David M. *A System architecture for Cyber Incident Mission Impact Assessment.* MS thesis, AFIT/GIR/ENV/08-M20. School of Systems and Engineering Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2008.

TexaSoft. (2008). *Interrater reliability (Kappa) Using SPSS*. Retrieved from: http://www.stattutorials.com/SPSS/TUTORIAL-SPSS-Interrater-Reliability-Kappa.htm

Thiem, Lisa S. *A Study to Determine Damage Assessment Methods or Models on Air Force Networks.* MS thesis, AFIT/GIR/ENV/05M-18. School of Systems and

Engineering Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2005.

Tinnel, L.S., Saydjari, O.S., & Haines, J.W. "An Integrated Cyber Panel System," *Proceedings of the 2003 DARPA Information Survivability Conference and Exposition, Vol. 2,* 32- 34, 2003.

Trochim, W.M. & Donnelly, J. P. (2008). *The Research Methods Knowledge Base* (3rd ed.). Mason, OH: Atomic Dog; Cengage Learning.

Vanbelle, S.& Albert, A. (2008). A note on the linearly weighted kappa coefficient for ordinal scales. *Statistical Methodology, 6*(2), 157-163. doi: 10.1016/j.stamet.2008.06.001

Ware, W. (1970). *Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security.* The RAND Corporation, Santa Monica, CA; February 1970.

Weber, R. P. (1990). *Basic Content Analysis* (2nd ed.). Newbury Park, CA: Sage Publications.

Wong-Jiru, Ann. *Graph Theoretical Analysis of Network Centric Operations Using Multi-layer Models.* MS thesis, AFIT/GSE/ENY/06-S01. School of Aeronautics and Astronautics, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, September 2006.

Vita

Biographical Sketch

Chief Master Sergeant Brian L. Hale grew up in Hartford, Wisconsin. He enlisted in the Air Force under the Delayed Enlistment Program in October 1984 and entered active duty on 8 August 1985 after graduating from Hartford Union High School. He completed technical training as an Administration Specialist and has built a vast breadth of experience during his career, serving at various levels, from detachment to Headquarters Air Force.

Chief Hale is currently a student at the Air Force Institute of Technology (AFIT) pursuing a Master of Science Degree in Information Resource Management. Prior to attending AFIT, Chief Hale was the Knowledge Operations Management (formerly Information Management) and Postal Air Force Career Field Manager, Washington DC. He oversaw training, manpower, utilization, assignments, and related actions involving 11,000 active duty, Guard, and Reserve knowledge operations management and postal authorizations.

Education

Master of Science, Information Resource Management, Air Force Institute of Technology, Wright-Patterson AFB, Ohio. Master’s Thesis: Mission Assurance—A Review of Continuity of Operations Guidance for Application to Cyber Incident Mission Impact Assessment (CIMIA). Chair: Michael R. Grimaila, PhD, CISM, CISSP. In progress. Expected graduation date: June 2010.

Bachelor of Science, Management/Computer Information Systems, Park University, St. Louis, Missouri, December 2004.

Standard Form 298 – Report Documentation Page

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 06/2010	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From – To)* September 2009 – June 2010

4. TITLE AND SUBTITLE Mission Assurance: A Review of Continuity of Operations Guidance for Application to Cyber Incident Mission Impact Assessment (CIMIA)	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Hale, Brian L., Chief Master Sergeant, USAF	**5d. PROJECT NUMBER** 10ENV297
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GIR/ENV/10-J01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Douglas Kelly, PhD, Cyber Team Lead Air Force Research Laboratory 711th Human Performance Wing Sense-making and Organizational Effectiveness Branch (RHXS) 2698 G Street, Bldg 190 Wright-Patterson AFB OH 45433-7604 Comm: (937) 656-4391	**10. SPONSOR/MONITOR'S ACRONYM(S)** AFRL/HPW/RHXS **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Military organizations have embedded information technology (IT) into mission processes to increase operational efficiency, improve decision-making quality, and shorten the sensor-to-shooter cycle. This IT-to-mission dependence can place the organizational mission at risk when an information incident (e.g., loss or manipulation of an information resource) occurs. Non-military organizations typically address this type of IT risk through an introspective, enterprise-wide focused risk management program that continuously identifies, prioritizes, and documents risks so control measures may be selected and implemented. The explicit valuation of information resources in terms of their ability to support the organizational mission objectives provides transparency and enables the creation of a continuity of operations plan. While this type of planning has proven successful in static environments, military missions often involve dynamically changing, time-sensitive, complex, coordinated operations involving multiple organizational entities. As a consequence, risk mitigation efforts tend to be localized. The research investigates the concept of mission assurance and presents a content analysis of existing continuity of operations elements within military and non-military guidance to assess the current policy landscape to highlight best practices and identify policy gaps in an effort to further enhance mission assurance by improving the timeliness and relevance of notification following an information incident.

15. SUBJECT TERMS

Mission Assurance, Continuity of Operations, Cyber Incident Mission Impact Assessment, Continuity Plan, Risk Management

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	18. NUMBER OF PAGES	**19a. NAME OF RESPONSIBLE PERSON** Grimaila, Michael R., PhD; AFIT/ENV
a. REPORT	b. ABSTRACT	c. THIS PAGE			**19b. TELEPHONE NUMBER** *(Include area code)*
U	U	U	UU	162	(937) 785-3636 x4800 (Michael.Grimaila@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18

	Form Approved *OMB No. 074-0188*