Software Engineering Institute

Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes

Richard A. Caralli
James. F. Stevens
Charles M. Wallen (Financial Services Technology Consortium)
David W. White
William R. Wilson
Lisa R. Young

May 2007

TECHNICAL REPORT
CMU/SEI-2007-TR-009
ESC-TR-2007-009

CERT Program

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

List of Tables

Foreword

In 2003, the Survivable Enterprise Management team at the Software Engineering Institute's CERT® Program set out to transform the way that organizations view and manage security. Since then, the term *security* has become obsolete for describing the tasks that organizations perform to protect the assets that are critical to their missions. We also found that security is difficult to define without reference to business continuity. Business continuity pertains to sustaining critical assets, and with security, forms a partnership that the organization relies on to manage operational resiliency.

This report is the third in a series that explores the transformation of the disciplines of security and business continuity into organizationally driven processes designed to support and sustain operational resiliency. In December 2004, we published a technical note entitled *Managing for Enterprise Security* that described the barriers that organizations face in making security an effective contributing factor to the achievement of organizational goals [Caralli 2004]. A subsequent technical note entitled *Sustaining Operational Resiliency: A Process Approach to Security Management* was published in April 2006 [Caralli 2006]. It expanded the description of the security discipline by linking it to activities such as business continuity and IT operations management. It also put forth the concept of operational resiliency as a process that can be defined, managed, measured, and improved.

This technical report is a refinement of the concepts included in these previous works and introduces the field of resiliency engineering—a process of collaboration between security, business continuity, and other organizational activities aimed at managing operational resiliency. A framework that defines the resiliency engineering process and establishes a process improvement approach is under development; this technical report lays the foundation for the framework and provides a high-level outline view of the existing framework body of knowledge.

We hope that organizations will be able to improve their security and business continuity efforts by focusing their activities and objectives toward the resiliency engineering process and by beginning to embrace a process improvement approach.

® CERT is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Acknowledgements

Many persons within and outside of the CERT Program have been instrumental to developing the concept of resiliency engineering and codifying the process definition that is presented as part of this report.

First and foremost, we would like to thank Rich Pethia, CERT program director at the Software Engineering Institute (SEI), and William Wilson, technical manager of the Survivable Enterprise Management (SEM) team, for their ongoing guidance and support of this important project. Their leadership continues to pave the way for delivering our message.

We would also like to thank members of the CERT Practices and Development Team, particularly Georgia Killcrece, Robin Ruefle, and Mark Zajicek, who have supported our work and have provided an internal forum for collaboration and discussion.

In addition, we would like to thank Howard Lipson from the Survivable Systems Initiative for his careful and thoughtful review of our work and his suggestions for improvements and future considerations.

Our external collaborators are a great source of wisdom and contribution to this work. Foremost, we would like to thank Charles Wallen, Managing Executive for Business Continuity at the Financial Services Technology Consortium (FSTC), whose leadership has brought valuable and knowledgeable people to the table from the best financial institutions in the world. Our work would not have advanced without their input, generosity, and patience. (In Appendix E, we provide a directory of these valuable contributors.) Specifically, the authors would like to thank Brad Mitchell of U.S. Bank for his extensive review of this document and thoughtful feedback.

And finally, as always, we are grateful to Pamela Curtis for her careful editing of this report and previous works that have resulted in the framework that is published as part of this technical report.

Executive Summary

The challenges to an organization's viability are numerous and rapidly escalating. Nearly every organization—commercial, government, or otherwise—finds itself in an operating environment that is increasingly hostile and uncharted. The quest to improve the organization's bottom line and increase value to stakeholders has brought with it a whole host of new hurdles that ironically can undo progress made through opening operational boundaries, installing technology pervasively, and distributing the workforce.

An organization's natural response to this challenging environment is to react—the equivalent of a "fight or flight" response. But reacting is a tacit admission by the organization that it cannot direct, control, and actively manage its operational environment. Reacting is an inefficient and ineffective approach to the challenges of the new world because it consumes more resources, pulls the organization's attention away from its core business drivers, and leaves the organization less capable in the long run. Instead of adopting the adage "What doesn't kill us makes us stronger," the organization becomes weaker because it doesn't create and nurture capabilities for navigating the risk environment it chooses to operate within.

Regulatory bodies have attempted to change the organization's proclivity for reacting by creating and imposing regulations and guidance. While this helps the organization to recognize the behaviors it needs to adopt and cultivate, it doesn't foster the development of a defined and manageable approach.

Unfortunately, the security and business continuity functions in the organization are often on the front line in dealing with the challenges of the new world. For the organization to be successful and viable in the long run, these functions must be directed toward improving and sustaining the organization's operational resiliency. Security and business continuity must evolve into activities that enable the achievement of organizational goals and the return of value to stakeholders rather than impede the organization's growth. To do this, the organization must manage, not react.

This report is the next evolution of thought regarding the coming of age of the security and business continuity functions: that security and business continuity are key contributors to operational resiliency, and that operational resiliency can be viewed as a process that can be managed and improved. We characterize this new vantage as the *resiliency engineering process* and seek in this report to introduce this field and lay the groundwork for a process framework, which is currently under development.

Requirements-driven security and business continuity characterize the resiliency engineering process. Thus, resiliency engineering is defined as the process by which an organization designs, develops, implements, and manages the protection and sustainability of business-critical services, related business processes, and associated assets such as people, information, technology, and facilities. And because the process can be defined, theoretically it can also be managed, measured, controlled, and improved, perhaps even optimized.

A process definition—one that can be used as a baseline for process improvement efforts—is being codified in the CERT Resiliency Engineering Framework. This framework will define the

competencies that an organization must master in order to manage operational resiliency.

As with engineering concepts, the application of process improvement methodologies outside of product development processes has been evolving. But, fundamentally, the concept behind process improvement—that a process that can be defined can be measured and managed—is applicable to other processes. In the case of resiliency engineering, this requires that the focus of process improvement move away from project-driven processes to enterprise processes that traverse the organization.

Because security and business continuity are fields often thought of as practice driven, the movement toward resiliency engineering provides an opportunity for an initial application of process improvement concepts. In essence, process improvement is introduced to security and business continuity through the definition of the resiliency engineering process.

Abstract

As security issues dominate news headlines and affect our daily lives, organizations need to improve their ability to protect and sustain their business-critical assets—people, information, technology, and facilities—using human and financial resources efficiently and effectively. Traditional activities such as security and business continuity must not only be effective at achieving these goals but also must offer the organization increased capabilities for managing and controlling operational resiliency. Unfortunately, organizations often manage these activities in a reactive posture fraught with stove-piped organizational structures and poorly defined and measured goals. The result: potentially less-than-adequate operational resiliency to support business objectives. But organizations can vastly improve operational resiliency by viewing it as an engineering-based process that can be defined, managed, measured, and improved. This view ensures collaboration between security and business continuity activities toward common goals and considers the role of supporting activities such as governance, asset and risk management, and financial control. This report introduces the CERT Resiliency Engineering Framework as a foundational model that describes the essential processes for managing operational resiliency, provides a structure from which an organization can begin process improvement of its security and business continuity efforts, and catalyzes the formation of a community from which further definition of this emerging discipline can evolve.

1 Introduction

Welcome to the new world. The challenges to an organization's viability are numerous and rapidly escalating. Nearly every organization—commercial, government, or otherwise—finds itself in an operating environment that is increasingly hostile and uncharted. The quest to improve the organization's bottom line and increase value to stakeholders has brought with it a whole host of new hurdles that ironically can undo progress made through opening operational boundaries, installing technology pervasively, and distributing the workforce.

An organization's natural response to this challenging environment is to react—the equivalent of a "fight or flight" response. But reacting is a tacit admission by the organization that it cannot direct, control, or actively manage its operational environment. Reacting is an inefficient and ineffective approach to the challenges of the new world because it consumes more resources, pulls the organization's attention away from its core business drivers, and leaves the organization less capable in the long run. Over time, the organization becomes less effective because it doesn't create and nurture capabilities for navigating the risk environment it chooses to operate within.

Regulatory bodies have attempted to change the organization's proclivity for reacting by creating and imposing regulations and guidance. While this helps the organization to recognize the behaviors it needs to adopt and cultivate, it often moves the organizational focus away from managing the operational environment to achieving compliance.

Unfortunately, the security and business continuity functions in the organization are often on the front line in dealing with the challenges of the new world. For the organization to be successful and viable in the long run, these functions must be directed toward improving and sustaining the organization's operational resiliency. Security and business continuity must evolve into activities that enable the achievement of organizational goals and the return of value to stakeholders rather than impede the organization's growth. To do this, the organization must manage, not react.

1.1 BACKGROUND

One of the goals of the CERT Survivable Enterprise Management team is to help organizations improve their capabilities and capacities to manage security activities in alignment with and support of strategic objectives. In our early work we focused on helping organizations to consider security as a business rather than technical function. Indeed, one of the drivers for the development of the CERT OCTAVE® risk assessment method was to involve business units in the information security process. At the business unit level, experience about how assets support business processes can be transformed into meaningful requirements for protecting and sustaining these assets. Thus, the business driver for security as an organizational competency was established.

As our work evolved, the foundational shift to security as a business problem led to the recasting of security as a fundamental operational risk management (ORM) activity. Clearly, the emerging organizational focus on managing operational risk (particularly in the banking and financial services industry) was instrumental in establishing the connection between security activities and operational risk management ob-

® OCTAVE is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. OCTAVE is the Operationally Critical Threat Asset and Vulnerability Evaluation. More information on this method can be found at http://www.cert.org/octave.

jectives. Further examination also established that security is but one function that contributes significantly to ORM—other activities such as business continuity management and IT operations and service delivery management also provide meaningful support for attaining operational risk management objectives.

Further examination of the security-ORM connection resulted in another key observation: the rationale for an organization's focus on managing ORM is to gain a level of control over operational resiliency—the organization's ability to adapt to risk that affects its core operational capacities. This led to a characterization of operational resiliency as an emergent property of effective and efficient operational risk management, supported and enabled by activities such as security and business continuity.

This report is the next evolution of thought regarding the coming of age of the security function: that security is a key contributor to operational resiliency, and that operational resiliency can be viewed as a process that can be managed and improved. We characterize this new vantage as the "resiliency engineering process" and seek in this technical report to define this field by providing a corresponding process definition and framework to continue the organizational transformation.

1.2 SHIFTING PERSPECTIVES

An overarching motive for the Carnegie Mellon® Software Engineering Institute's (SEI's) continuing work in this area is to help organizations to identify and overcome fundamental barriers that impede the evolution of security and business continuity into operational risk management and operational resiliency-driven activities. For example, basic needs, such as the alignment of all risk-based activities to a common set of organizationally driven risk drivers, are missing in many organizations. This leads to silos where activities such as security and business continuity do not intentionally intersect, and if they do, it is because of overlapping activities (such as business impact analysis) and not because of well-planned and executed coordination toward the goal of sustaining operational resiliency. This also reinforces the perception of senior management that security and business continuity are necessary evils that are funded because of uncertainty and fear or out of a need to comply rather than because they enable the organization to meet strategic objectives.

For an organization to effectively evolve its security and business continuity activities and overcome these barriers, it must embrace four fundamental assertions:

1. Security and business continuity are enterprise processes, owned and managed by the organization and focused more broadly than just on technology.
2. Security and business continuity are fundamental contributors to the organization's operational risk management process, with the ability to control and actively manage operational resiliency as the goal.
3. The process for managing and sustaining operational resiliency is characterized by an organizationally focused process called *resiliency engineering* that involves competencies that are performed throughout the enterprise.
4. The resiliency engineering process can be defined, managed, measured, and improved through the application of process improvement tools, techniques, and methodologies.

This report specifically focuses on the latter two assertions by defining and describing the resiliency engineering process in a framework for process improvement.

® Carnegie Mellon is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

1.3 OPERATIONAL RESILIENCY AS THE GOAL

Operational resiliency is a property that emerges from the activities that an organization performs to keep services, business processes, and assets viable and productive under changing risk conditions. It describes the organization's ability to adapt to and manage risks that emanate from day-to-day operations. An organization that has resilient operations should be able to systematically and transparently cope with disruptive events so that the overall ability of the organization to meet its mission is minimally or not adversely affected. Traditional activities such as security and business continuity are in reality focused on sustaining operational resiliency.

At the center of operational resiliency is operational risk management. Operational risk is the risk that arises from day-to-day operations. It is an unpleasant reality inherent in the activities the organization performs to meet its mission. Operational resiliency is directly affected by how well the organization manages operational risk, which is the foundation of security and business continuity activities. Thus, operational resiliency emerges when security and business continuity are successful in helping the organization to manage operational risk. As a result, many aspects of operational risk management can be found throughout our approach to resiliency engineering.

Neither security nor business continuity activities alone can bring about operational resiliency. Instead, it requires a collective focus on organizationally derived risk drivers that align with business objectives. Security and business continuity management must collaborate to ensure that the organization achieves an effective level of operational resiliency at the most efficient cost.

Figure 1 provides a graphic description of the foundation for operational resiliency.

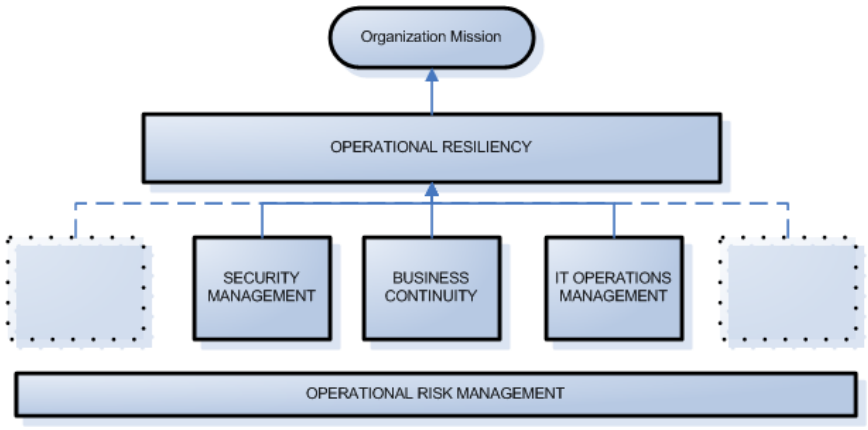


Figure 1: Foundation for Operational Resiliency

(This technical report does not discuss this topic at length. For a more detailed discussion about operational risk management and operational resiliency, please refer to the technical note entitled *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* [Caralli 2006].)

1.4 INTRODUCING RESILIENCY ENGINEERING

Engineering is a discipline that involves the application of art and science to the design, planning, construction, and maintenance of a manufactured object [Encarta 2006]. Engineering as a practice is often thought of as applicable only to physical goods and products (such as cars and buildings), but there has been much support for extending and applying basic engineering practices to the design and production of nonmaterial objects such as software and systems.

To say that something has been "engineered" is to imply that a systematic process of design and construction originating from defined requirements has been undertaken. Requirements are the foundation of all engineering-based processes, and the result of an engineered process is a product or service that substantially meets or exceeds all of the requirements that are established. Requirements also form the basis for managing operational resiliency. The protection and continuity needs of an asset are based on resiliency requirements that reflect how the asset is used to support the organization's strategic objectives. When these requirements are not met through security and business continuity activities, the operational resiliency of the asset is diminished, and one or more of the organization's strategic objectives fails to be met. Operational resiliency depends on establishing requirements in order to build resiliency into assets and services and to keep these assets and services productive in the accomplishment of strategic objectives.

Requirements-driven security and business continuity characterizes the resiliency engineering process. Thus, resiliency engineering is defined as the process by which an organization designs, develops, implements, and manages the protection and sustainability of business-critical services, related business processes, and associated assets such as people, information, technology, and facilities. And because the process can be defined, theoretically it can also be managed, measured, controlled, and improved, perhaps even optimized.

For more than two years, we have been investigating, accumulating, and codifying a resiliency engineering body of knowledge. Section 2 of this report describes the basic concept of resiliency engineering.

1.5 IMPROVING PROCESSES

Defining the concept of resiliency engineering is not sufficient to help an organization transform from a security and business continuity perspective to one that is focused on resiliency and strategic objectives. While it provides a common understanding of the tasks that an organization must perform to manage operational resiliency, a simple definition of the resiliency engineering process will not provide sustainable process management and improvement. This is the domain of a process improvement approach.

The origins of process improvement can be traced traditionally to product-based manufacturing processes. Processes are defined and variation to these processes that results in unplanned outcomes is identified and addressed.

As with engineering concepts, the application of process improvement methodologies outside of product-focused development processes has been evolving. The suite of capability maturity models at the SEI is viable proof of the extensibility of process improvement techniques across a wide range of engineering disciplines. But, fundamentally, the concept behind process improvement—that a process that can be defined can be measured and managed—is applicable to other processes. In the case of resiliency engineering, this requires that the focus of process improvement evolve away from project-driven processes to enterprise processes that traverse the organization. Because security and business continuity are fields often thought of as practice driven, the movement toward resiliency engineering provides an opportunity for an initial application of process improvement concepts. In essence, process improvement is introduced to security and business continuity through the definition of the resiliency engineering process.

1.6 SCOPE OF THIS REPORT

This report intends to accomplish several objectives:

- Continue to build on earlier work in enterprise security management and operational resiliency management.

- Describe the emerging field of resiliency engineering and define and describe basic resiliency engineering concepts.
- Define the resiliency engineering process and introduce a process improvement framework.
- Discuss the rationale for and the potential benefits of the application of process improvement methodologies to resiliency engineering.
- Establish a common language for resiliency engineering and resiliency engineering process improvement.
- Establish a dialog with the community for input to the development of an eventual process improvement model.

1.7 STRUCTURE OF THE REPORT

The sections of this document are arranged by the objectives of the report as follows:

- Introduction and background – Section 1
- Resiliency engineering definition and concepts – Section 2
- Resiliency engineering in practice – Section 3
- Moving toward model-based process improvement – Section 4
- Looking forward to the CERT Resiliency Engineering Framework – Section 5
- Beginning a process improvement effort – Section 6
- Value proposition for financial institutions – Section 7
- Future direction and research – Section 8

1.8 TARGET AUDIENCE

The target audience for this technical report is people and organizations who have an interest in adopting a model-based process improvement approach to managing and improving operational resiliency and, by extension, their security and business continuity processes. Knowledge of the concepts of operational risk management, operational resiliency, and process improvement is helpful to understanding the emerging field of resiliency engineering. Those who have process improvement experience will begin to recognize the initial application of these concepts to managing operational resiliency and the resiliency engineering process.

Before reading this technical report, it may be helpful to familiarize yourself with previous work that we have completed that has led up to this work. This can be found in the technical notes *Managing for Enterprise Security* [Caralli 2004] and *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* [Caralli 2006] as well as other documents and presentations in the "Security and Resiliency Engineering" section of the CERT "Organizational Security" portal at www.cert.org.

2 Resiliency Engineering

Imagine that you are asked to build a bridge across a body of water. How do you proceed? Do you gather together some materials and people and begin to construct the bridge? If you want the bridge to be functional, structurally sound, and durable, of course the answer is "no."

A bridge, like any physical structure, is built through a systematic and disciplined process—by defining requirements, creating the approach and design, procuring materials and labor to meet the requirements, establishing a construction plan, and executing tasks against the plan. But these are only the most obvious tasks. Many other activities must be performed—funding for the bridge is secured, budgets for design and construction tasks are created and funded, legal permits are filed, relevant regulations are identified and complied with, accounting and reporting is performed to ensure the project is on track, requirements are revisited and managed as construction conditions dictate, and updated skills and training are provided to people as needed to ensure that what is built meets what has been requisitioned and designed.

Building a bridge clearly requires the coordination of many different skill sets and contributions toward a common goal: a bridge that meets requirements within the allocated budget and in the time period expected. Reacting to the request to build the bridge without planning, controlling, directing, and managing the effort could lead to a disaster.

Managing operational resiliency requires a similar systematic and disciplined approach. It must flow from requirements that represent the needs of the organization and form the basis for protecting and sustaining critical assets and services. The organization must perform security and business continuity tasks under the constraints of changing requirements, limited funding, regulatory demands, accounting and budgeting requirements, and availability of skilled labor. Disparate parts of the organization must coordinate their work to make the organization adaptable to known and unknown risks that can steer it off course and impede accomplishment of the mission. In short, the organization must learn to be capable in managing operational resiliency across the enterprise rather than to react to disruptive events.

An engineered process provides a level of control over the outcome of the process. If the organization's goal is to ensure that critical business processes and services meet their mission, the way to achieving that goal is through definable and repeatable processes that can be improved and optimized over time. Thus emerges the concept of resiliency engineering—the process by which an organization designs, develops, implements, and manages the protection and sustainability of business-critical services, related business processes, and associated assets such as people, information, technology, and facilities. In other words, resiliency engineering is the way that the organization builds in and manages resiliency, rather than bolting it on.

2.1 FOUNDATION FOR RESILIENCY ENGINEERING

What matters most for an organization is that the key business processes and services it performs are able to meet their missions consistently, within budgeted costs, and within operating tolerances. This simple but important goal is the foundation for resiliency engineering. This section describes the concept of resiliency engineering and establishes a foundation for a process improvement approach to resiliency engineering.

2.2 RESILIENCY ENGINEERING OBJECTS

The focus of operational resiliency is the organization's services, related business processes, and asso-

ciated assets. Collectively, the operation of these organizational resources propels the organization to achieve its mission.

The relationship between services, business processes, and assets and their importance to resiliency engineering is described in the following sections.

2.2.1 Services

The highest order object in the definition of the resiliency engineering process is a service. Services are defined as the limited number of activities that the organization carries out in the performance of a duty or in the production of a product. Services can have an internal focus (such as the hiring of staff or the payment of invoices) or, more commonly, an external focus (such as producing a car or offering a service such as washing cars). A service that is actively in production is considered to be operative or "in operation."[1]

A service is the highest level concept in resiliency engineering. An organization has a limited number of services that it performs. Traditionally, services align with an organization's lines of business (LOB). For example, an integrated energy company may produce natural gas, transport it, and distribute it to consumers. Production, transportation, and distribution can be viewed as "services" that the organization performs.

Services are the prime resource that the organization uses to accomplish its mission. Each service has a mission that must be accomplished in order to support the organization's strategic objectives. Failure to accomplish the mission of a service is a potentially serious impediment to accomplishing the organization's mission. For example, the inability to transport natural gas due to the loss of SCADA[2] system functionality directly impedes the mission of an integrated energy company.

A service in production is supported by the execution of one or more business processes as depicted in Figure 2.

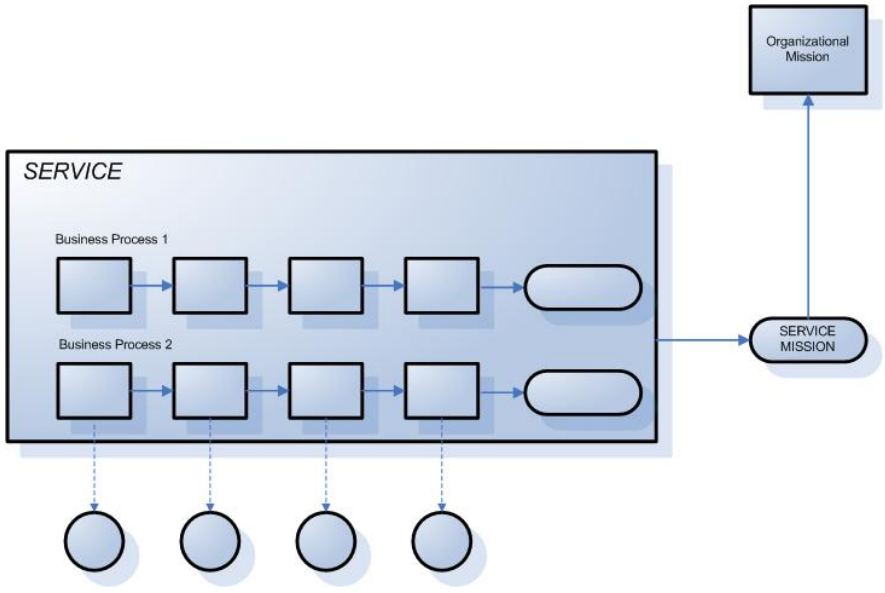


Figure 2: Graphic Depiction of a Service

[1] A service that is actively in production—that is, fulfilling a duty or producing a product—is considered to be in operation. Thus, in the resiliency-engineering concept, *operations* is defined as the productive activity of services.

[2] SCADA is an acronym for Supervisory Control and Data Acquisition. SCADA systems help an organization to manage and measure the flow of natural gas across pipelines from production points to distribution points.

2.2.2 Business Processes

Business processes are activities that the organization (and its suppliers[3]) performs to support the achievement of the mission of one or more services. A business process is composed of one or many separate activities that must be executed sequentially to be successful. The mission of a business process must support the mission of a service. In other words, business processes enable services to meet their mission, which in turn supports achievement of strategic objectives.

Business processes are pervasive. An organization may have hundreds or thousands of business processes that directly or indirectly support one or more services. As a complicating factor, many business processes are not performed entirely by the organization. They may be outsourced entirely or the organization may receive help from suppliers on one or more activities that compose a business process. Failure of one or more business processes can affect the ability of one or more services to meet their missions. Figure 3 provides a graphical depiction of the relationship between services and associated business processes.

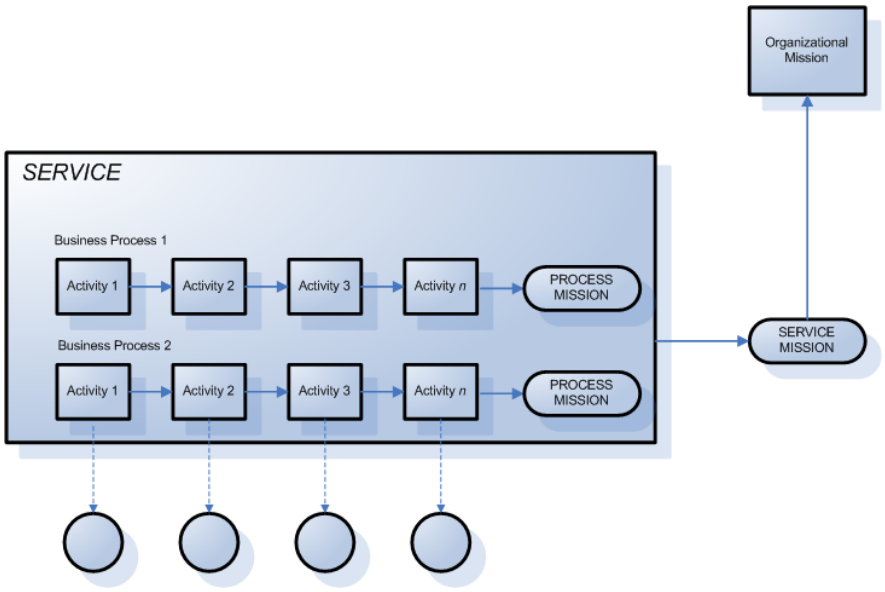


Figure 3: Graphic Depiction of a Service and Related Business Processes

An important aspect of business processes is that they are "fueled" by assets—the raw materials that the process needs to operate. In other words, a business process generally cannot accomplish its mission unless there are

- *people* to operate and monitor the process
- *information* and data to feed the process and be produced by the process
- *technology* to automate and support the process
- *facilities* in which to perform the process

2.2.3 Assets

Assets are something of value to the organization. Assets are charged into production to facilitate the effective and efficient operation of business processes and services. The value of an asset is relative to the

[3] A supplier is a business partner who supplies key products and services to the organization to contribute to accomplishing the missions of business-critical processes.

importance of the asset in supporting critical business processes and services. For example, an organization's customer database is important because it may be used to create customer invoices, record sales leads and activities, and produce customer communications. The loss of this database disrupts the operation of many services and business processes.

There are four types of assets that must be considered in the resiliency engineering process: people, information, technology, and facilities.

People

People are the human capital of the organization. There are few services and business processes that operate without human intervention, either in an active manner or in a monitoring capacity. People use other assets—information, technology, and facilities—to achieve goals.

The requirement of *availability* is the primary consideration for the operational resiliency of the "people" asset. The organization must enable people to be available and to stay as productive as possible in carrying out their responsibilities for supporting services and business processes.

Information

Information is quickly becoming the most pervasive organizational asset. The shift of an organization's asset portfolio from tangible to intangible assets is due to the increasing value of and reliance on information. Business processes and services require information to operate. For example, customer invoices cannot be produced without customer information, product information, prices, or payment terms.

An information asset is any data that is important to the organization. Information can take many forms, both tangible and intangible. It can be raw data that requires significant processing to be usable to the organization, or it can be the organization's intellectual property such as proprietary methodologies, formulas, or strategic plans. Information can also be found in many places in the organization. People know information that is important to the organization (generally called "knowledge"); information is stored on technical assets such as servers and personal computers; and file rooms are full of paper-based information that is written, printed from application systems, or on other media such as microfiche.

The requirements of *confidentiality, integrity, and availability* are all relevant considerations for the operational resiliency of the "information" asset. The organization must protect information that is limited to a need-to-know basis, ensure that information is not altered in a way that makes it unusable, and ensure that information is available in the form intended and required for use in business processes and services.

Technology

Technology is also a pervasive organizational asset. Few organizational services are untouched by some aspect of technology—hardware, software, systems, tools, and infrastructure (such as networks and telecommunications infrastructure)—that supports services and business processes. Technology assets directly enable the automation (and efficiency) of business processes and services. For some organizations, technology is a prominent driver in accomplishing the mission and is considered a strategic element. Technology tends to be pervasive across all functions of the organization and therefore can be a significant contributor to strategic and competitive success.

The requirements of integrity and availability of technology assets are relevant for the operational resiliency of "technology" assets. The organization must ensure that technology remains in the condition required to support services and business processes (which is generally accomplished through integrity-focused tasks such as configuration, change, and release management) and is available when needed.

Facilities

People, information, and technology objects "live" within a physical facility—people work in offices (or at home), information is stored in file rooms or on servers, and technology is housed in specialized facilities such as data centers.

Organizations may not always have direct control over the facilities where their services and business processes are executed or their assets are located. Facilities may be owned by the organization, but frequently they are acquired or leased from another organization. These arrangements sometimes also mean that the organization's assets are co-located with those of other organizations in the same facility. This presents challenges not only for facilities management but also for ensuring the operational resiliency of services that depend on these facilities to meet their missions.

The requirements of integrity and availability are relevant for considering the operational resiliency of "facility" assets. Organizations must ensure that facilities are usable as designed and maintained and that they are available when needed to support the execution of services and business processes.

Figure 4 shows a notional relationship between services, business processes, and related assets.

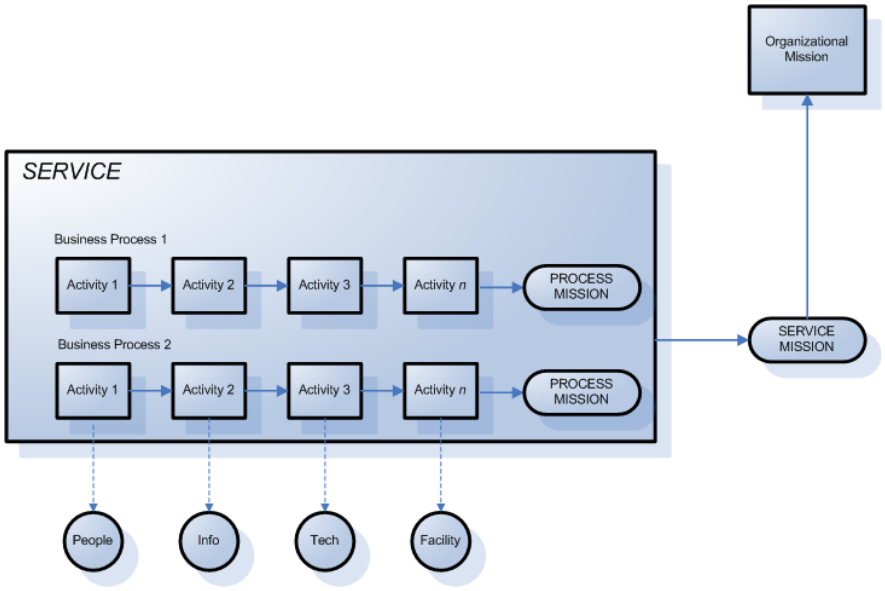


Figure 4: Graphic Depiction of Services, Business Processes, and Assets

3 Resiliency Engineering in Practice

The focus of resiliency engineering is the active management and control of operational resiliency. Operational resiliency is a property that emerges from the activities that the organization performs to keep services, business processes, and assets viable and productive under changing risk conditions. In other words, resiliency engineering is the process that the organization uses to protect services, business processes, and assets from threats and make them sustainable whenever they are affected by a disruptive event.

3.1 FUNDAMENTAL CONCEPTS

Resiliency engineering in practice requires a reference definition of the resiliency engineering process. This definition is based on several key concepts. They include

- the connection between service and asset resiliency
- a focus on requirements as the catalyst for the process
- optimizing between protection and sustainability strategies
- coverage of the entire asset life cycle

Each of these is explained in more detail in the following sections.

3.1.1 Service Resiliency Starts with Asset Resiliency

Services "consume" assets in the pursuit of their missions.[4] Assets only have meaning when they are charged into the production of a service or a business process. If an asset doesn't support the achievement of a service or business process goal, it may not have appreciable value to the organization.[5]

Potential risks to the organization are generally targeted at the disruption of an asset. For example, if a hacker wants to take down a critical organizational service such as a web portal, the attack is perpetrated on the technology assets (network, servers) or information assets (customer database). Thus, the operational resiliency of services and business processes is directly linked to asset resiliency. This creates a "house of cards" that the organization must actively manage. Failure in a critical asset can cascade into the failure of one or more services and business processes, and eventually, the organization finds its productivity is diminished, its goals are unattainable, and its reputation is diminished. This is often the case with facility assets—the loss of a facility generally materializes in the degradation or termination of many diverse business processes that the organization "feels" in the form of potentially lost sales, increased production costs, diminished health and safety of employees and customers, legal fines and penalties, lawsuits, and other areas of impact. Consider the impact on the organization if it loses a data center—many significant processes come to a halt along with the operating capacity of the organization.

Organizations generally take a service or business process view of resiliency (particularly at the operating

[4] This concept is analogous to the way that assets are used in a production cycle. Assets are charged into production as raw materials to produce a product. In the same way, assets such as people, information, technology, and facilities are used to support the production of business processes to achieve their intended outcome—whether to produce a product or provide a service.

[5] This is not to say that the assets that are the focus of the resiliency engineering process are the only ones that must be protected and sustained. For example, if an organization loses significant financial assets (such as cash, equities, or bonds), it may not be able to accomplish its mission. However, the protection and sustainability of financial assets would be the focus of financial risk management as a part of overall enterprise risk management. The assets of resiliency engineering are those that are subjected to operational risk and are directly related to the productive capacity of the organization.

unit or line of business level) but often forget to consider the dependency on assets. For example, an organization may state that its web portal must be available 20 hours a day and six days per week, but to be achievable, this target must translate into specific resiliency requirements (that meet or exceed service requirements) for all assets that the service depends on. Thus, true service resiliency is dependent on the cumulative effect of asset resiliency and considerations of resiliency at the asset level. Unless an organization takes a balanced view of the resiliency of services and assets (that is, in consideration of service and asset dependencies), operational resiliency cannot be managed effectively.[6]

3.1.2 Requirements Are the Catalyst

The importance of requirements to the resiliency engineering process cannot be understated. Resiliency requirements embody the strategic objectives, risk appetite, critical success factors, and operational constraints of the organization in its pursuit of the mission. They represent the alignment factor that ties practice-level activities performed in security and business continuity to what must be accomplished at the service and asset level in order to move the organization toward its mission.

In terms of practical application, a resiliency requirement is a constraint that the organization places on the productive capability of an asset to ensure that it remains viable and functional when charged into production to support a service or business process. For example, Table 1 outlines basic resiliency requirements for paper-based medical records (an information asset) in a physician's office. These records are essential to the provision of high-quality medical services to patients on demand, and a failure to meet these requirements potentially interferes with their effective use as intended in providing these services.

Table 1: Example of Resiliency Requirements

- *Confidentiality*
  - Patient medical records may be viewed only by office physicians, physician assistants, and nurses.
  - Patient medical records of a specific patient may be viewed by that patient (or their authorized representative) upon his or her request.
- *Integrity*
  - Additions to patient medical records may be made only by office physicians, physician assistants, and nurses.
  - Modifications of existing patient medical information may be made only by physicians, or by physician assistants and nurses *on the approval of an attending physician.*
  - Deletions of existing medical record information may be made only by a physician.
  - Existing patient medical records may be destroyed only on the approval of a physician.
- *Availability*
  - Patient medical records must be available during normal office hours (9:00 am to 5:00 pm, Monday through Thursday, and 10:00 am to 6:00 pm on Saturdays).
  - Patient medical records must be available on demand when physicians need them for attending to patients.

Thus, resiliency requirements are a derivation of the traditionally described security objectives of confidentiality, integrity, and availability. Confidentiality, integrity, and availability are well known by the se-

[6] While it is common for organizations to become myopic about resiliency at the service level, the opposite can often be true as well—organizations that focus solely on operational resiliency at the asset level may lack an appreciation of how asset resiliency affects business processes and services. This can also be a barrier to managing operational resiliency effectively.

curity community as descriptive properties of information assets, but their application from a resiliency perspective is extensible to the other types of assets with which resiliency engineering is concerned. Table 2 describes the extension of resiliency requirements to assets other than information.

Table 2: Extension of Resiliency Requirements to all Types of Resiliency Assets

Resiliency Requirement	Asset Type			
	People	Information	Technology	Facilities
Confidentiality	--	✓	--	--
Integrity	--	✓	✓	✓
Availability	✓	✓	✓	✓

The extension of these requirements to assets other than information is well established in the security and business continuity domains. For example, security activities are normally focused on protecting against the unauthorized or inadvertent disclosure of information and the prevention of unauthorized or accidental modification of information, technology assets (in the form of configurations), and facilities (in the form of physical structures and access controls). Business continuity activities, on the other hand, are primarily focused on ensuring the availability of these assets when affected by a disruptive event. Together, these practitioner-level activities address the range of resiliency requirements that are necessary to manage operational resiliency. In fact, the satisfaction of resiliency requirements at the asset level is where security and business continuity make their contributions to the control and management of operational resiliency.

Resiliency requirements provide the basis for how assets are protected and made sustainable so that they can perform their intended duties in support of services and business processes. Resiliency requirements become a part of an asset's DNA (just like its definition, owner, and value) that transcends departmental and organizational boundaries—it goes with the asset wherever it lives. Resiliency requirements also drive or influence many of the competencies in the definition of the resiliency engineering process. For example, resiliency requirements

- form the basis for developing controls and protection strategies for assets (controls management)[7]
- form the basis for developing continuity of operations plans for assets (sustainability management)
- reflect the compliance and regulation requirements of the organization[8] (compliance management)
- reflect the risk appetite of the organization (risk management)
- are included in the service-level agreements of asset custodians, including suppliers (supplier agreement and relationship management)
- provide the validation factor for access controls and privileges (access control management)
- affect the day-to-day resilient management of assets—people (human resources management), information (knowledge and information management), technology (technology management), and facilities (environmental control and facilities management)

[7] Parenthetical references are to areas of competency that form a baseline process definition of the resiliency engineering process.

[8] For example, the data privacy provisions of the Health Insurance Portability and Privacy Act (HIPPA) of 1996 would be incorporated into the confidentiality requirements for medical records.

3.1.3 Optimizing Between Asset Protection and Sustainability

Operational risk management is a significant influencing factor in resiliency engineering. The identification, analysis, and mitigation of operational risk are the means by which the organization controls and manages operational resiliency. While resiliency engineering does not encompass or describe all of the tasks of operational risk management, the resiliency engineering process clearly contains a strong risk management basis for many of the related competencies and practices.

The basic risk equation—a condition plus a consequence—is reflected throughout the resiliency engineering philosophy (Figure 5). At the asset level, practical application of resiliency engineering concepts involves two basic activities: managing *conditions* that could pose risk to the asset and managing the sustainability of an asset to limit or prevent *consequences* to the organization as a result of realized risk. The basic risk equation requires the organization to optimize its approach between condition management and consequence management to provide the overall most effective (and cost-efficient) level of asset resiliency possible.

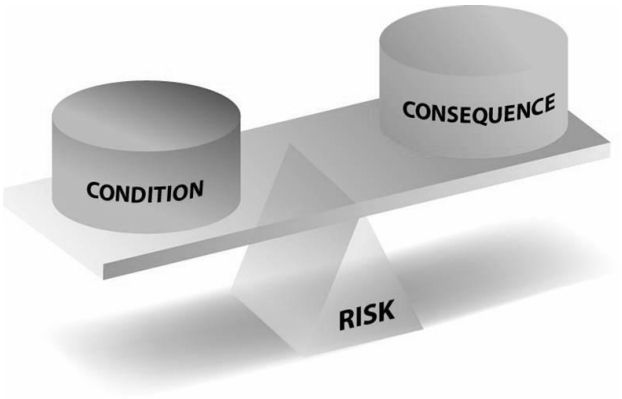


Figure 5: Basic Risk Equation

The optimized approach must also consider how the asset is used—what service and business processes does the asset support and enable and what are the resiliency requirements of the asset? Optimizing the mix between these two activities for the overall good of the asset and its associated services is a difficult task.

The application of the risk equation to the operational resiliency of assets results in two basic resiliency engineering tasks—asset protection and asset continuity, or "protect and sustain" for short. These activities, when optimized and made congruent with the resiliency requirements of the asset, form a resilient shell around the asset. Figure 6 depicts operational resiliency at the asset level.

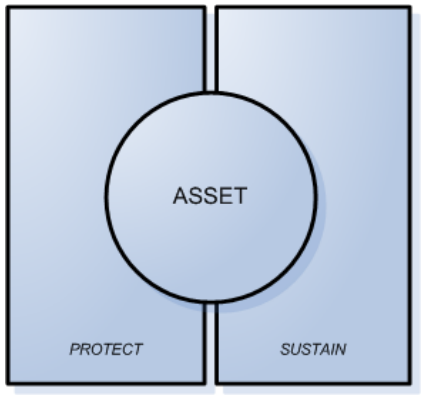


Figure 6: Operational Resiliency at the Asset Level

This concept for operational resiliency captures the basic premise of risk management—not all risk can be identified or eliminated, thus the organization must also be prepared to make the asset sustainable in case a risk is realized or new risks emerge, as well as to limit or manage any resulting impact to the organization. This concept also supports the need for collaboration between security and business continuity activities toward a common goal of operational resiliency. Security activities help the organization to protect assets by identifying threats and vulnerabilities and by implementing controls that prevent these threats and vulnerabilities from being acted upon, with the intention of preventing consequences to the organization as a result of realized risk. Business continuity or continuity of operations planning (COOP), on the other hand, is a sustaining activity. It focuses on identifying the services and assets that are most valuable to the organization and ensuring that plans are constructed and tested to provide continuity to the services and assets given numerous possible disruptive events, as well as to manage the effects of realized consequences on the organization. Both activities, in theory, should be aligned with the same risk drivers that the organization uses to manage other types of risk such as business risk, market risk, and credit risk.

Figure 7 depicts the relationship between operational resiliency, risk management, and the focus of security and business continuity activities.

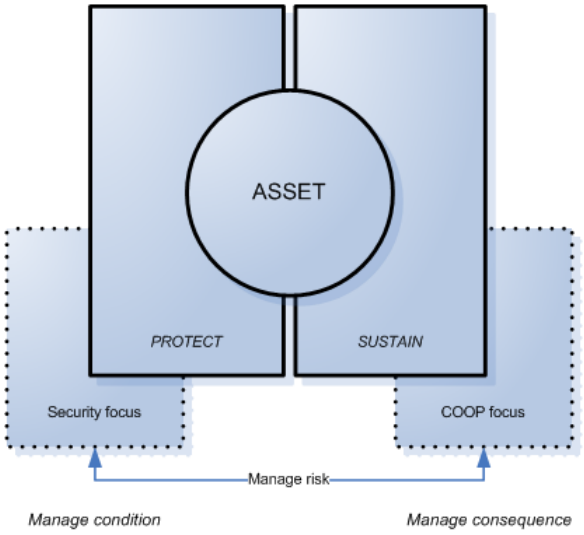


Figure 7: A Cooperative Approach to Operational Resiliency

The challenge for the organization is to strike an organizationally aligned, cost-efficient, optimized balance between the two strategies. Optimization requires more than just balancing controls against continuity of operations plans; it requires careful consideration of resources, applicable laws and regulations, other compliance commitments, and other issues such as training. For example, an organization with unlimited human and financial resources has less incentive to optimize these strategies because it can essentially replicate all of its critical functions so that when one is lost, the people, information, technology, and facilities needed to restore the functionality are immediately available. This is impractical for most organizations, and thus they must engineer an optimized strategy that works within constraints, financial or otherwise.

Finally, for resiliency engineering to have meaning at the enterprise level, this asset-level focus must be extensible to the service level. The optimization of protection versus sustainability for an asset strongly depends on how the asset operates or is charged into production to support a service. Conversely, the resiliency of a service is a function of the cumulative effect of the resiliency of the assets that support it. Thus, the connection between assets and services cannot be broken when addressing operational resiliency.[9]

3.1.4 Coverage of the Asset Life Cycle

The word *operational* in the phrase *operational resiliency* can be misleading. To suggest that an organization manages operational resiliency by focusing on assets and services only when they are in operation shortchanges the true value and extent of an engineered approach. Engineering is concerned with the proper design and construction of assets so that they are maintainable when implemented and operational. This same concept extends to a basic philosophy of resiliency engineering—that many of the issues that affect the operational resiliency of assets are inherited from inadequate considerations of resiliency earlier in the life cycle of asset development and acquisition. Thus, asset resiliency requirements are not only functional as a basis for optimizing protection and sustainability strategies for assets in operation, but they also guide the organization in developing and implementing these strategies *before* assets are implemented, whether developed or acquired. In fact, earlier consideration and satisfaction of requirements is the preferred approach in resiliency engineering because it significantly narrows the asset's operational risk environment.

[9] It is important to note that the role of a service may shift as a result of changes in the strategy or mission of the enterprise or in response to certain events. When this occurs, the role of an asset supporting the service may also change, resulting in a need to adjust the protection and sustainability strategies for the asset.

4 Moving Toward Model-Based Process Improvement

Model-based process improvement means simply that—using a model to guide the improvement of an organization's processes [Ahern 2004]. In some industries, such as software engineering, model-based process improvement is a way of life rather than an evolutionary concept. However, model-based process improvement is a promising approach for managing operational resiliency and the resiliency engineering process because it gives organizations a foundation and structure for improving and maturing resiliency processes through measurement of process capability, the identification of performance gaps, and the development and implementation of action plans to close the gaps.

Many organizations are simply not ready to take on process improvement. It requires commitment, a long-term view, and strong management support [Ahern 2004]. It also requires fundamental changes to be made in the way that the organization approaches work. This is a true hurdle for the security and business continuity community. Well-established organizational structures, funding models, and corporate cultures continue to impede sustainable improvement, as does the pervasive management perception that these activities are complex and technical in nature and are sources of costs that must be controlled rather than investments that add to the bottom line.

As organizations increase their exposure to new risk environments in a quest to find new sources of revenue and growth, current approaches to managing operational resiliency will become increasingly obsolete. Model-based process improvement may provide the structure, discipline, and sustainable basis for organizations to realize their goals.

4.1 A PROCESS DEFINITION FOR RESILIENCY ENGINEERING

A process[10] is a structured collection of related activities aimed at reaching a desired outcome. When a process has been designed, documented, and communicated, it can be used by an organization as a reference for carrying out the essential tasks needed to ensure that the desired outcome is reached.

The most fundamental reality about a process is that it binds together the three critical resources or dimensions needed for an organization to improve itself: people, procedures and methods, and tools and equipment, as shown in Figure 8 [Chrissis 2003].

[10] Process is used in this context as a higher order concept. For example, the software engineering process (which represents many sub-processes and practices) is of a higher order than a business process that maps a structured way to process an expense report or to produce a payroll.

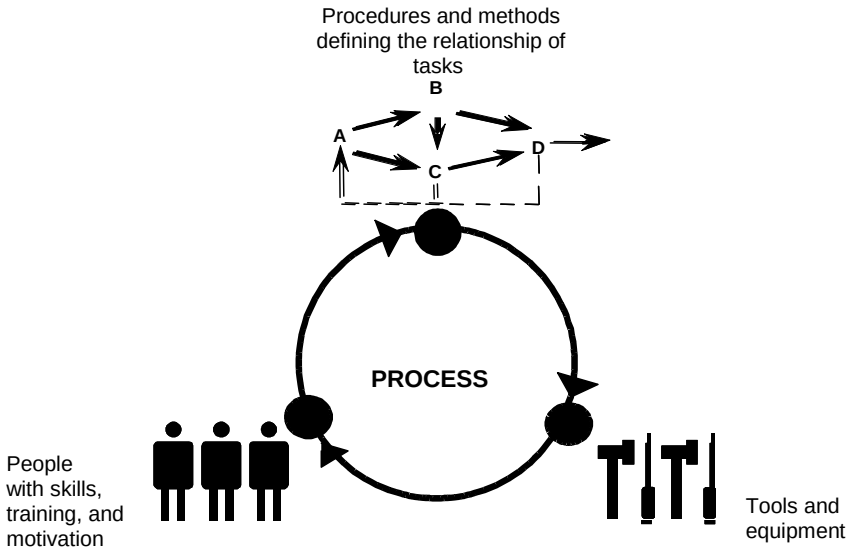


Figure 8: The Three Critical Dimensions of Improvement

Although this description has its origins in the software and systems engineering disciplines, it supports the challenge of managing operational resiliency as well. An organization must have defined procedures and methods, deploy people effectively, and master the use of tools and equipment to manage operational resiliency. But a process view captures the dependencies among these dimensions, and the lack of process is a significant reason why improvement in managing operational resiliency (and the supporting activities of security and business continuity) has been elusive.

4.1.1 Process Definition

A process can be described in a process definition.[11] A process definition is a description of the essential elements of a process that can be used to support communication and process improvement and management and to provide guidance for process performance and execution. A process definition can also form the basis for a reference model from which organizations can assess their current competencies in managing a process and set a target for future improvement.

Developing and using a process definition is a relatively new and evolving concept for the security and business continuity disciplines and for application to managing operational resiliency. In addition to catalyzing process improvement, a process definition also provides a foundation from which the security and business continuity communities can evolve and transform.

An initial process definition for the resiliency engineering process is documented in the CERT Resiliency Engineering Framework, which is introduced later in this document.[12]

---

[11] The body of knowledge for process definition, modeling, and improvement is vast. This report is not intended to represent this body of knowledge. This information is being presented as a primer for understanding the application of process improvement concepts and techniques to fields such as security and business continuity through the definition of the resiliency engineering process. The Software Engineering Institute (http://www.sei.cmu.edu) is a source and repository of significant information in the field of process improvement and can be used to improve understanding of essential process concepts.

[12] A process and its definition are the focus of a process model. A process model is the keystone of a process improvement approach and contains not only the process definition but guidance for improving processes through process goal achievement and practice adoption. We consider the CERT Resiliency Engineering Framework to be an early version of a process model.

4.1.2 Practice Versus Process

To understand process definition and how it is used in a process improvement approach, it is important to distinguish *process* from *practice*. In its basic sense, a practice is something that is done habitually in order to attain a skill. In application, a practice is a prescriptive way of doing something that leads to an intended result. Process differs significantly from practice. A process is a descriptive device. It defines *what* is to be done, not *how*. Practices align to processes because they are the way that the organization achieves the *what*.

In their current state, security, business continuity, and the management of operational risk and resiliency are highly practice-oriented disciplines. Thus, practices form the substance of how organizations manage these disciplines. But this does not put the focus on higher level process goals that, when achieved, are a better indication of organizational competency. A practice focus detracts security and business continuity activities away from consideration of service and business process mission achievement and thus contributes to the lack of appreciable improvement in the management of operational resiliency and the alignment of security and business continuity to strategic objectives.

This is not to say that the use of practices is ill advised. Practices generally reflect the collective experience of a community or industry and thus can help an organization to quickly improve an activity by taking advantage of the experience of its peers. However, because of their prescriptive nature, practices tend to mislead organizations into believing that once they have been implemented, no further attention to them is necessary. And practices are rarely, if ever, assessed for sustainability; that is, organizations do not often assess whether practices are sustainable over time such that the organization's successes are consistently and reliably able to be repeated.

A process definition by nature is a reference against which practices can be assigned. Through a process improvement framework, the process definition provides a descriptive structure to which the right prescriptive best practices can be implemented, integrated, and managed. And, while the process definition may remain fairly static over time, it allows for the fact that practices may change drastically, usually through the advancement of new techniques, tools, and methods and the innovations of people. Figure 9 provides a notional example of how security, business continuity, and IT operations practices can relate to a single competency area.

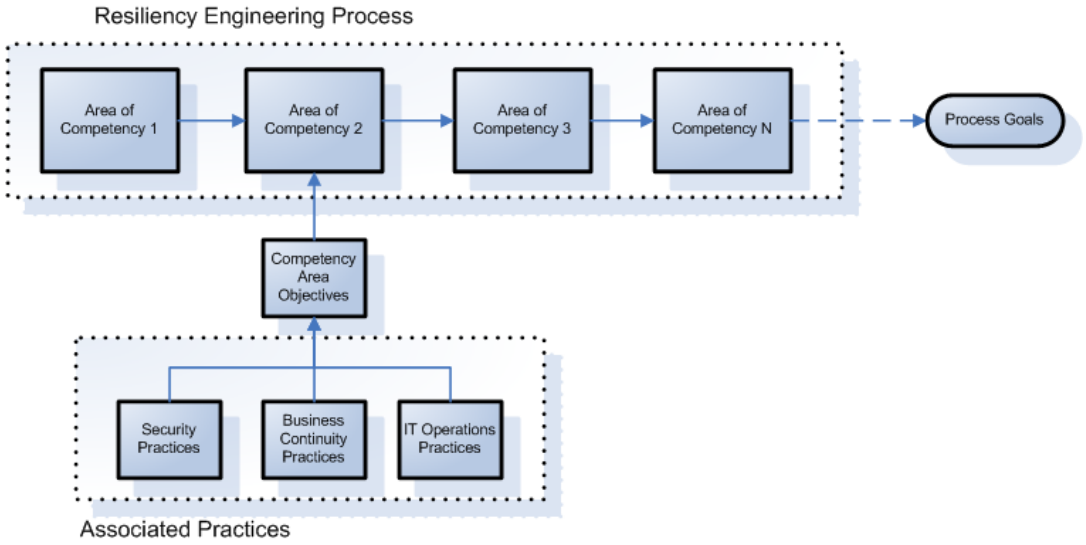


Figure 9: Process Versus Practice

4.2 BENEFITS OF A MODEL-BASED PROCESS IMPROVEMENT APPROACH

A model-based process improvement approach is meant to help an organization work smarter, not harder. Models provide the organization a common set of process requirements that reflect best practices and can be used to guide the process improvement efforts of the organization in a way that suits its operational constraints [Ahern 2004]. Models provide discipline and they help the organization to improve the consistency of results and goal attainment. Models also give the organization a baseline from which to evolve from immature processes and practices to mature processes that encompass improved quality and effectiveness [Chrissis 2003].

Specifically, considering a model-based process improvement approach to resiliency engineering has value and provides certain benefits. Sections 4.2.1 and 4.2.2 highlight the value proposition and outline the potential benefits of the proposed CERT Resiliency Engineering Framework.

4.2.1 Generic Benefits of Using a Process Improvement Approach

Common process definition

A process definition is the foundation of a process approach. It codifies a shared description of a process that can be communicated, understood, and implemented by those who are responsible for achieving the goals of the process. It also lays the groundwork for process management and measurement.

A common process definition can also reduce the ambiguity and vagueness that result from traditionally ill-defined processes. Security, for example, means different things to different people and organizations. A process definition of operational resiliency that properly positions security activities can serve as a means to reduce this ambiguity. It also lays the foundation for future improvement because it provides a common understanding that can be discussed, debated, and revised.

Common language

A common and sharable process definition brings a common language that can further reduce ambiguity and improve understanding and assimilation. This is important not only for the organization itself but also in communications with suppliers, vendors, customers, regulators, and any external person or organization that needs to avoid issues that result from getting "lost in translation." A common language also helps an industry or emerging community to grow because language does not become an inhibitive barrier.

Consistent benchmark for measurement

A common process definition and language are essential for establishing a competency benchmark. Organizations want to know how they are performing in a particular process relative to their peers, their industry, and perhaps even their competitors. A consistent benchmark that reflects the community and industry's best practices can be a powerful tool for providing information on current performance, potential gaps, and strengths and weaknesses relative to other organizations.

Benchmarking can also strengthen an entire industry. For example, it can provide a way to communicate with regulators and lawmakers. Rather than developing and implementing regulations to force acceptable behaviors, a common benchmark for achievement and measurement can give regulators a tool to examine industry performance and allow them to focus on problem areas that need to be addressed.

Potential for independent, third-party appraisal

The ability to benchmark performance against a common process definition also has the potential to provide the foundation for independent third-party appraisals of competency. While many organizations will be able to objectively self-assess their performance, an independent appraisal gives them another tool in

improving processes. Independent appraisals provide objective information on where process improvement should begin. They can also show an organization how current practices integrate into the process definition.

A valuable benefit of independent appraisals is the ability of an organization to know with reasonable certainty the competency of its business partners in managing operational resiliency. The *resiliency value chain*—the chain of suppliers, internal or external to the organization, that must be resilient in order to ensure that a business process or service meets its mission—can be improved by identifying the strengths and weaknesses of suppliers and by helping the organization to proactively choose suppliers that align with its philosophy on managing operational resiliency. This also reduces the need to make decisions based on subjective data and unsubstantiated claims.

Over time, independent appraisals can also help a process improvement community to develop, collect, and share trend and process improvement data, which can be used to sustain process improvement efforts.

Catalyze a process improvement community

All of the aforementioned benefits of model-based process improvement are important for bringing together a community focused on sharing process improvement knowledge, tools, techniques, and methodologies. A strong community can help to mature the process improvement model and ensure that it reflects not only current best practices but that it evolves as new and emerging practices and challenges become known.

4.2.2 Benefits of a Process Improvement Approach to Operational Resiliency

Consistent risk drivers

One of the most significant barriers to managing operational resiliency is the inconsistent application and communication of risk objectives, tolerances, and appetite throughout the enterprise.

Risk management is an activity that pervades all organizational layers. Everyone in the organization who is responsible for managing some type of risk—business, financial, market, or operational—must act on the same organizational assumptions; otherwise, the organization's overall ability to identify and mitigate risk is impaired. In practical terms, this characterizes the conflict between security and business continuity activities—using different risk assumptions and risk measurement criteria results in conflicting risk priorities and resulting mitigation actions. Failing to use the same risk drivers as the basis for risk activities impedes a holistic approach to risk management at the asset level.

Focus on strategic objectives

An organization performs services and business processes to satisfy strategic objectives and pursue its mission. To support this goal, organizations may implement elaborate performance management processes to ensure that every level of the organization supports the achievement of one or more strategic objectives—in essence, the organization engineers an approach for accomplishing its mission.

The focus on strategic objectives is a guiding factor for the resiliency engineering process as well. Accomplishing strategic objectives in an effective and efficient way is the justification for investment in operational resiliency—for developing and implementing controls; developing, testing, and executing continuity of operations plans; and ensuring the availability of people, information, technology, and facilities. When resiliency requirements reflect the importance of assets, business processes, and services in supporting strategic objectives, managing operational resiliency becomes a fundamental means of achieving these objectives.

Potential to eliminate redundancy and cost

The costs of managing operational resiliency continue to grow as organizations encounter new and increasingly unfamiliar risk environments. This results in mounting pressure to obtain funding (and to find new sources of funding) but also to be more cost effective and responsible in the ways that these funds (and other resources) are used.

A process view forces the organization to look at process outcomes as the basis for making rational decisions regarding the optimal deployment of resources. For example, if the organization is suffering the impact of undetected incidents, it can examine its incident and vulnerability management processes, measure accomplishment of process competency objectives in these areas, and determine what changes it needs to make. This forms a rational basis for resource requests because they are tied to reducing process achievement gaps that must be closed to improve operational resiliency.

A process view makes current funding models for operational resiliency activities obsolete. Instead of funding activities based on departmental operations or lines of business, operational resiliency management is funded through an enterprise-driven strategy. This also mitigates potential overspending that typically accompanies large-scale disruptive events or crises that are funded based on reaction and emotion rather than on a carefully directed and executed plan.

The cost of resiliency management should be a function of process achievement, not department goals and budgets or disruptive events. Antiquated funding models mean that the organization may be over-supporting some activities and under-supporting others—in other words, failing to optimize protection and sustainability strategies. Without looking at resiliency engineering at a process level, however, the organization has difficulty in determining where these inequities exist and where duplicative costs can be eliminated. Through a process view, the organization gets a clearer and more comprehensive picture of what needs to be funded, to what extent, and how.

Process is measurable and manageable

The ability to extract cost from managing operational resiliency and bring value to the organization is dependent on being able to measure the effectiveness and efficiency of the resiliency engineering process.

Organizations have become complacent in accepting the absence of data as a measurement of effectiveness of risk management activities.[13] Therein lies the advantages of a process view—a process that can be defined can also be measured, controlled, and managed. While metrics in some fields such as security are still a subject of contention, a process view at least forces the organization to define initially what *can* be measured and to measure it on a regular basis.[14] And it focuses the measurement on the process, not the practice. It allows the organization to identify gaps in expected performance, which can then be prioritized and corrected. What is learned in measurement can be fed back into the process for improvement, allowing for goal achievement that is systematic and more disciplined than it is in most organizations today. Organizations are not left to wonder whether their investments have value or whether the end results of their processes are achieved—they can measure them.

---

[13] For example, the lack of organizational impact from a known event or incident may be seen as a confirmation of the effectiveness of the organization's ability to manage operational resiliency.

[14] The ability to convert these concepts to the resiliency engineering process should not be trivialized. The development of metrics and measurement of success will be more difficult than it is in other disciplines such as software engineering. For example, reducing defects to 15 per 100,000 lines of software code is a significant and tangible result that can be directly attributable to improved software engineering processes. It is hoped that metrics of this type in resiliency engineering (such as reduced downtime of technical assets) can result from moving to a process view.

Guided practice selection and implementation

A process perspective turns the organization's focus to the *outcome* of the process. Through a process improvement framework, a process view provides a descriptive structure in which the *right* prescriptive best practices for the organization can be implemented and integrated because it forces the organization to consider whether the practices it selects and implements will drive it toward process competency target achievement. With a process view, an organization is less likely to fall into a "set it and forget it" approach because the success of the process is actively dependent on the practices that are implemented to support it. Because the *process* is the guide, there is less need to be concerned with implementing a particular body of practices to achieve adequate coverage because what needs to be achieved is defined by the process, not the practice body. Thus, inadequate or ineffective practices are weeded out and practices are selected on the basis of how they support process competency objectives.

Improved organizational value

What could an organization do with improved operational resiliency? For one thing, it could have more control over meeting its operational goals with improved certainty and less disruption. It may also be able to redirect resources to their most efficient deployment. With confidence, the organization may be poised to grow new lines of business and enter new marketplaces where unknown risks may have previously scared it away.

An organization with control over operational resiliency provides a level of comfort and confidence to potential shareholders, current stakeholders, regulators, and customers. It has the potential to become the supplier of choice because customers have improved confidence in its ability to stay viable during disruptive events that affect the supply chain. Improved control over operational resiliency may also translate into lower cost to customers because typically "hidden" costs are being identified and driven out through improved process management.

Improved customer value, a higher level of trust and confidence, and improved position in the marketplace are all possible benefits of a process improvement approach that, until now, may not have been conceivable, let alone achievable.

A roadmap for maturing processes

One of the challenges for security or business continuity is the ability to sustain competency and success. The organization's current practices may appear to be effective in managing the protection and sustainability of critical assets and business processes, but the accomplishment may be temporal. As conditions in the operational environment change, the organization may not be able to sustain its competency or repeat its success because it has not established the institutionalizing structures and practices that it needs to mature processes. In other words, the organization may be successful today under today's conditions but may not be doing enough to ensure that success can be repeated in a sustainable way over time. Such is the problem with point-in-time security assessments or business impact analyses—the organization may look competent under current conditions, but there is no measurement of its long-term capabilities. Only when the organization makes a commitment to improving and maturing processes can there be any real indication of how it will perform under times of stress, across multiple lines of business, or when it grows. Thus, its capability for long-term success becomes a more meaningful measure of competency.

A process improvement model provides the organization a roadmap for improving and maturing its resiliency engineering processes. As the organization moves away from simply satisfying basic goals and practices toward higher levels of process management and maturity, it is investing in successively higher levels of competency to the extent needed to meet its unique business challenges and strategic objectives.

4.3 APPLYING THE CONCEPTS OF PROCESS MATURITY

It is difficult, if not impossible, to address the concept of process improvement without addressing *process maturity*. Indeed, a fundamental selling point of models such as the SEI CMMI® framework is the ability to describe an evolutionary path of process maturity that an organization can use as a benchmark and a structure for process improvement.

Unfortunately, process maturity, particularly in the security and business continuity space, is vastly misunderstood, and resulting maturity models are generally poorly executed. Instead of describing a predefined roadmap for organizational improvement based on proven grouping and ordering of processes,[15] many of these models simply group performance criteria into levels, provide descriptive titles for those levels, and present the result as a maturity model. The problem with this approach is that there is rarely an underlying process description on which maturity is based, and descriptions of process maturity (as linked to the process definition) are absent. At best, what results is a descriptive notion of increasing levels of performance but not an evolutionary path of process maturity.

Another problem in applying process maturity concepts in the security and business continuity discipline is the propensity to view the outcomes of the process as guaranteed. For example, process maturity in security processes does not necessarily imply that the organization is secure—it only implies that the organization has the *capability* to secure itself. Models that attempt to bring maturity concepts to security and business continuity often forget this simple fact.

Our proposed resiliency engineering framework does not address process maturity, if only because there is little existing evidence to support a staged maturity representation. However, it does serve as the foundation for future consideration of process maturity, and there is at least anecdotal evidence of process maturity that begins to emerge from consideration of the practices that can be tied to each competency area in the framework. However, this does not mean that process maturity should be ignored—it must be explored and researched, and a good way to start is to determine how maturity characterizations and levels in other models might be adapted to "fit" the resiliency engineering process.

4.3.1 Understanding Process Maturity

Process maturity affects the architecture of a process improvement framework or model. For example, the SEI CMMI framework provides guidance for two representations of its model: staged and continuous. A staged representation provides a prescriptive roadmap for improvement based on grouping process areas[16] and ordering processes in a way that has been proven to help organizations make marked improvements [Ahern 2004]. A continuous representation differs in that there is less prescription about how to approach process improvement and there are no "discrete stages" through which the organization proceeds. Instead, the continuous representation allows for improvement of individual capabilities in an order relevant to the organization that is taking on process improvement [Ahern 2004].

Both or either of these representations could be useful and necessary constructs for describing process maturity as applied to the resiliency engineering framework.

® CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

15 This is the definition of a staged maturity model [Ahern 2004].

16 A process area is a grouping of like topics or aspects of a larger process. For example, Requirements Development is a process area in CMMI. Each process area has a set of goals and specific practices that comprise the essential activities of the process area. In the CERT Resiliency Engineering Framework, process areas are called competency areas.

4.3.2 Describing Process Maturity for Resiliency Engineering

In our initial research, we have found that there is value in being able to express resiliency engineering process maturity in terms of a continuous representation. In CMMI, this means that process maturity is described for each process area through capability levels [Chrissis 2003]. Each capability level describes an incremental improvement in the organization's process maturity within a process area.

There are six capability levels that can be described for any process area in CMMI: incomplete, performed, managed, defined, quantitatively managed, and optimizing.

Level 0 – Incomplete

Level 0 represents a process that is either not performed or is partially performed [Chrissis 2003]. Thus, the basic process definition for the process area is not adhered to and the goals of the process are not achieved. This may indicate that the organization performs this process in an ad hoc, reactive manner and is dependent upon competent people to achieve success.

Level 1 – Performed

In Level 1, a process is performed by satisfying the goals of the process area [Chrissis 2003]. Thus, the process exists and is performed by the implementation and execution of activities, tasks, and practices that support goal achievement. There is no indication of whether the organization can sustain this performance over time or whether this performance is consistent.

Level 2 – Managed

In Level 2, processes are considered to be "managed" [Chrissis 2003]. A managed process is one that has the necessary infrastructure in place to support the process. For resiliency engineering, this means that in addition to achieving the competency objectives of the process there is governance and oversight over the process, skilled people are assigned to and responsible for the process, the process is adequately funded, and relevant stakeholders of the process are identified and involved.

Thus, "managed" resiliency engineering processes are those that are not only performed but are actively supported, reviewed, governed and monitored, instantiated in policy, and controlled. A movement from level 1 to level 2 represents an enormous leap for the competencies defined in resiliency engineering—in level 2, the structure and discipline required to achieve the competency begins to become institutionalized, and the evolution from an unmanaged, reactive discipline to one that is manageable, controllable, and predictable is commenced.

Level 3 – Defined

Level 3 builds on level 2 as processes are not only managed but also defined. In CMMI, *defined* refers to establishing and maintaining a consistent definition of a process that is tailored from the organization's set of standard processes [Ahern 2004]. This allows the organization the flexibility it needs to consistently meet high-level resiliency engineering process improvement goals while allowing for differences in the way that things are done across organizational units, lines of business, divisions, or companies. Level 3 also introduces the collection of measurement data to support process improvement efforts. For resiliency engineering, this level represents the movement to qualitative and quantitative expressions of process achievement that can replace an organization's propensity to define success in vague, immeasurable, and unverifiable terms.

Levels 4 and 5 – Quantitatively Managed and Optimizing

Levels 4 and 5 in CMMI represent the movement toward process performance management and process

optimization. Unfortunately, there are few existing examples of organizations that are truly quantitatively managing or optimizing security and business continuity processes—in our experience, many are barely covering the range of practices that have been collected in the resiliency engineering body of knowledge. However, levels 4 and 5 provide a glimpse into the future direction of the resiliency engineering process improvement movement—to be able to use quantitative measures and methods to make the organization more resilient and to sustain it at a level of resiliency commensurate with the achievement of strategic objectives.

Improved process quality, improved innovation, and foundational support for strategic objectives are not just important to building software or systems—they also matter for activities like security and business continuity, which are not generally viewed as contributing to the mission of the organization. A movement toward defining and achieving similar concepts for resiliency engineering is not a matter of if, but when.

5 Looking Forward to the CERT® Resiliency Engineering Framework

The CERT® Resiliency Engineering Framework will be the first step in the development of a process improvement approach to operational resiliency management. It provides a baseline process description of the competencies required to manage operational resiliency and, by default, to focus security and business continuity activities on organizationally driven objectives.

5.1 FRAMEWORK SCOPE

The scope of the framework is broad because an organization's operational capacities span the enterprise. Thus, the enterprise is the focus of the resiliency engineering framework. As a result, the description of resiliency engineering process covers many diverse activities that span the organization and often extend beyond the organization. These activities are not typically considered as part of the scope of security and business continuity.

The scope of the framework also covers the various aspects of an asset's life cycle—from requirements definition, to design and development, to implementation and operations and maintenance—and is inclusive of the range of activities that traditionally represent security and business continuity activities, as well as relevant IT operations and service delivery activities.

5.1.1 Covering the Asset Life Cycle

Although the resiliency engineering framework has an operational focus, its coverage extends to earlier phases of an asset's life cycle. This is because an organization's operations generally inherit the effects of poor resiliency decisions made (or not made, as the case may be) early in the development of assets. Thus, an important objective of the framework is the movement of resiliency decisions to the earliest point in the development, acquisition, and implementation of assets and services. This should result in more effective management of operational risk and resiliency, as well as improved control of costs and resources.

While this is a concept most often associated with the development of software and system assets, it is extensible to information asset design and acquisition as well as the design, development, and construction or the acquisition and leasing of facility assets.

5.1.2 One Framework Versus Two

The framework covers more than security and business continuity activities. Operational resiliency management also requires excellence in IT operations and service delivery management and relies on core competencies that support the organization's ability to achieve its business objectives. For example, enterprise-level activities such as governance, risk management, financial management, and organizational training are all significant contributors to improving and sustaining operational resiliency, and for improving process maturity.

The framework eliminates the need for separate security and business continuity process models. Frameworks focused on security or business continuity alone are limiting because separately these activities do not ensure operational resiliency; only when they are part of a larger enterprise-wide effort do they effectively support organizational drivers and shared risk assumptions. Building separate frameworks would engender the failure to share requirements, drive toward common goals, or reduce redundancy and cost in

the effort to boost operational resiliency. In other words, separate frameworks would further ingrain the silo-like nature of these activities as they exist in most organizations today.

The following sections provide background information on the proposed objectives, structure, and architecture of the framework.

5.2 FRAMEWORK OBJECTIVES

The CERT Resiliency Engineering Framework is being developed to meet a number of diverse objectives with the intention of addressing the barriers and impediments of improving operational resiliency, the symptoms of which have been documented in this technical report and previous works.

In summary, the objectives for developing the framework include

- helping organizations to redefine and refocus security and business continuity efforts and achieve process improvement while driving out costs
- documenting a baseline process definition for managing operational resiliency
- adapting and applying process improvement concepts and methods to the management of operational resiliency
- providing a reference model from which a resiliency engineering process improvement community can evolve
- laying the foundation for integration to other process improvement models that do not specifically focus on the enterprise

5.2.1 Process Versus Checklist Approach

The framework proposes to codify a set of high-level processes (through the concept of competency areas) rather than an itemized checklist of characteristics or criteria against which the organization assesses itself. Establishing performance criteria may help an organization to reflect on how well it stacks up compared to the criteria, but once this diagnosis is completed, the organization is left without a roadmap to improvement. And a criteria-based approach by nature does not reinforce the need to mature practices so that success is sustainable. In fact, a process-based approach is what the organization needs to *satisfy* the criteria and to keep its performance consistent over the long term. The security and business continuity fields are fraught with criteria-based approaches, which may explain why real process improvement has been elusive.

5.3 STRUCTURE OF THE FRAMEWORK

The CERT Resiliency Engineering Framework is being developed using the structure of existing process improvement models in the public domain. This approach was chosen for two reasons:

1. It takes advantage of proven structures for documenting and communicating a process definition.
2. It provides a familiar structure for those who are already users of existing process models and facilitates transition, adoption, and integration by established communities of practice in process improvement.

Although the CERT Resiliency Engineering Framework is being developed at the Software Engineering Institute, it should be noted that it is not considered a part of the SEI's Capability Maturity Model® Integration (CMMI®) framework and is not intended to be integrated with existing CMMI models.

® Capability Maturity Model Integration and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

5.3.1 Framework Components

The resiliency engineering framework has several key components. At the highest level, it is composed of over 20 competency areas that define the major areas of activity that define resiliency engineering.

A competency area is an area of practice that the organization must master to some degree to manage operational resiliency. Competency areas are arranged into four competency categories. (More information on these categories is provided in Section 5.4.)

Each competency area has several standard components: competency objectives, associated practices, and subpractices. A competency area objective is a definition of what must be accomplished by the process. Each competency area has one or more competency objectives that must be attained.

A competency objective is attained through the implementation of high-level practices. Practices are descriptions of activities that are considered important in achieving the competency objectives to which they are associated and to which subpractices can be integrated. Subpractices can be high level as well, but most often represent best practices that are commonly used by an industry or community at the practitioner level.

5.4 FRAMEWORK ARCHITECTURE

The proposed architecture of the CERT Resiliency Engineering Framework is arranged in four categories:

1. Enterprise Management
2. Engineering
3. Operations
4. Process Management

These categories represent the broad range of activities that are important to managing operational resiliency. However, because resiliency engineering is a process that traverses the organization and is dependent on cooperation and coordination, these categories serve only as a way to group competencies by their common elements and focus. In reality, there is extensive interaction between competencies, and thus, the categories provide a foundation from which interaction can be performed.

The following sections describe the competency categories and examples of the types of competency areas that would be included in each category.

5.5 ENTERPRISE MANAGEMENT

The enterprise is an important concept in the resiliency engineering process. At the enterprise level, the organization establishes and carries out many activities that the resiliency engineering process relies on. In addition, it provides the enterprise focus that risk management activities must have.

The competencies in the Enterprise Management category represent functions and activities that are essential to supporting the resiliency engineering process. These competencies are typically representative of broad organizational competencies and functions that support many diverse activities. They are essential to managing operational resiliency because they explicitly connect the enterprise to the resiliency engineering process.

5.5.1 Enterprise Management Competencies

The competencies that represent the Enterprise Management category include

- EF – Enterprise Focus

- COMP – Compliance Management
- FRM – Financial Resources Management
- RISK – Risk Management
- COMM – Communications Management
- OTA – Organizational Training and Awareness

The current body of knowledge for Enterprise Management competencies is included in Appendix A.

5.6 ENGINEERING

The management of operational resiliency is a requirements-driven engineering function. Thus, the competencies in the Engineering category represent those that are focused on establishing and implementing resiliency for organizational assets, business processes, and services. These competencies establish the basic building blocks for resiliency and create the foundation for the protection and sustainability of assets, business processes, and services.

Engineering competencies can be described as falling into three broad categories:

1. *Requirements management* addresses the development and management of the security and resiliency objectives for assets and services.
2. *Asset management* establishes the important people, information, technology, and facilities assets across the enterprise.
3. *Establishing and managing resiliency* addresses the selection, implementation, and management of preventative controls and the development and implementation of impact management plans and programs.

The current body of knowledge for Engineering competencies is included in Appendix B.

5.6.1 Engineering Competencies

The Engineering competencies include

Requirements Management

- RRD – Resiliency Requirements Development
- RRM – Resiliency Requirements Management

Asset Management

- ADM – Asset Definition and Management

Establishing and Managing Resiliency

- SM – Sustainability Management
- CM – Controls Management

5.6.2 Important Engineering Competency Relationships

There are two important clusters of related competencies in the Engineering category: the asset cluster and the relationship between CM – Controls Management and SM – Sustainability Management. These relationships are explained in the following sections.

Asset cluster

The asset cluster forms a significant component of the resiliency engineering framework. The asset cluster

is focused on the identification of people, information, technology, and facility assets, and the change management activities that must be in place to ensure that the assets of the organization are known to the organization at any point in time. In addition, the asset cluster represents the resiliency activities that need to be performed for each of the asset types.

In the resiliency engineering framework, assets are identified and managed in the ADM – Asset Definition and Management competency area, and the resiliency considerations of each type of asset are addressed respectively as follows:

- People: HRM – Human Resources Management and OTA – Organizational Training and Awareness
- Information: KIM – Knowledge and Information Management
- Technology: TM – Technology Management
- Facilities: ECFM – Environmental Control and Facilities Management

This is depicted in Figure 10.

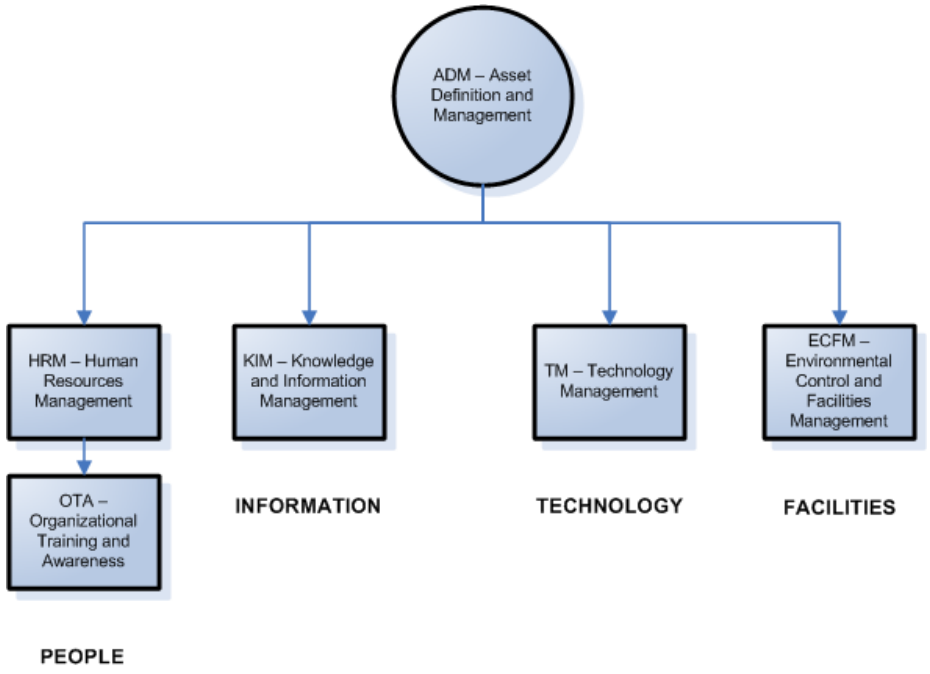


Figure 10: Asset Resiliency Management Cluster

In each of the competency areas that address asset resiliency, there is a standard structure that represents the competency objectives included in the competency area. For each asset-specific competency area, competency objectives and practices are included that represent the

- selection of a subset of assets (in each asset category) that are critical to the organization
- development and implementation of protective controls for assets currently in production and those that have not yet been developed or acquired
- identification, analysis, and mitigation of risks that are specific to the asset type
- consideration of resiliency-specific activities for each asset type based on the types of resiliency requirements that are specific to the asset type (for example, consideration of integrity and availability requirements for technology assets)

While this results in some overlap in content with competencies such as ADM – Asset Definition and

Management and CM – Controls Management, it provides a more robust consideration of the total scope of activities that must be performed at the asset level for operational resiliency.

5.6.3 Relationship Between Controls Management and Sustainability Management

The competency areas of CM – Controls Management and SM – Sustainability Management have a relationship that reflects the basic premise of the resiliency engineering process—the need to approach assets from a holistic risk view by considering protection strategy alongside continuity strategies to provide the best, most cost-efficient, overall strategy for keeping the asset resilient.

The failure in managing operational resiliency—and to some degree, operational risk—in many organizations is the lack of coordination between these processes. This is often institutionalized by having these functions performed in different parts of the organization while competing for the same limited resources.

Operational risk management and operational resiliency require the organization to ensure that the risk drivers that are considered important to the achievement of strategic objectives also guide the development and implementation of protection and sustainability strategies so that assets are made resilient commensurate with organizational needs. The coordination between Controls Management and Sustainability Management is intended to impose a holistic view of risk and resiliency management at the asset level, as illustrated in Figure 11.

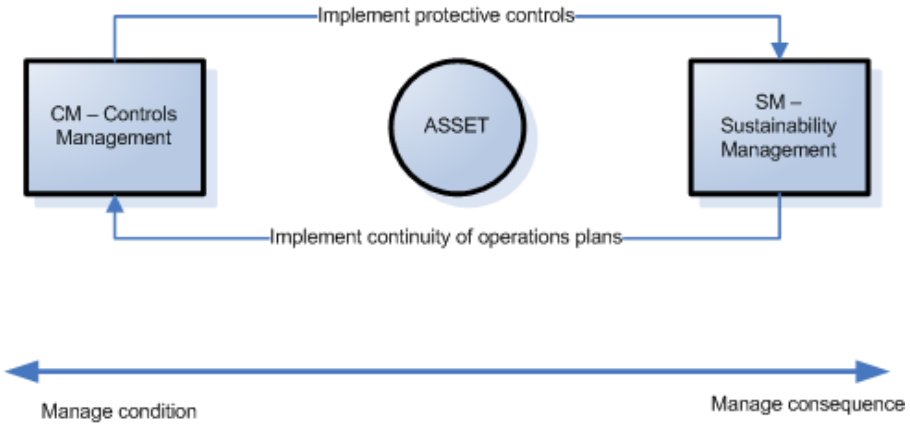


Figure 11: Protect and Sustain Cluster

5.7 OPERATIONS

The Operations competencies represent the core activities for managing the operational resiliency of assets and services. These competencies are focused on sustaining an adequate level of operational resiliency as prescribed by the organization's strategic drivers, critical success factors, and risk appetite. These competencies represent core security, business continuity, and IT operations and service delivery management activities and focus on the resiliency of information, technology, and facilities assets.

Operations competencies can be expressed as falling into four broad categories:

1. *Sourcing* addresses the management of organizational suppliers and the potential impact on the organization's operational resiliency.
2. *Threat, vulnerability, and incident management* addresses the organization's continuous cycle of identifying and managing threats, vulnerabilities, and incidents to minimize organizational disruption.

3. *Asset resiliency management* addresses the asset-level activities that the organization performs to manage operational resiliency of people, information, technology, and facilities to ensure the sustainability of business processes and services.
4. *Security operations management* addresses the day-to-day activities that the organization performs to protect the organization's technical and physical infrastructure.

The body of knowledge for Operations competencies is included in Appendix C.

5.7.1 Operations Competencies

The Operations competencies include

Supplier Management

- SAM – Supplier Agreement Management
- SRM – Supplier Relationship Management

Threat and Incident Management

- VM – Vulnerability Management
- IMC – Incident Management and Control
- AMC – Access Management and Control

Asset Resiliency Management

- HRM – Human Resources Management
- ECFM – Environmental Control and Facilities Management
- KIM – Knowledge and Information Management
- TM – Technology Management

Security Operations Management

- SOM – Security Operations Management

5.7.2 Important Operations Competency Relationships

There are two important clusters of related competencies in the Engineering category: the *supplier* cluster and the *vulnerability, incident, and risk* cluster. These competency relationships are explained in the following sections.

Supplier cluster

Most organizations do not possess (or want to possess) core competencies in all of the activities that they have to perform to sustain a growing business or to produce services and products. Organizations frequently acquire and develop relationships with external business partners—often referred to as *suppliers*—to provide these core competencies. However, these relationships can increase operational risk—the extent to which the organization allows suppliers to play a critical role in business processes and services affects the operational resiliency of those processes and services. Thus, the organization must ensure that suppliers understand and are willing to satisfy the resiliency requirements established by the organization for critical assets and services that it entrusts to their care. This is accomplished in the CERT Resiliency Engineering Framework through two competency areas: SAM – Supplier Agreement Management, where agreements and relationships are established, and SRM – Supplier Relationship Management, where performance

against requirements is managed, as shown in Figure 12.[17]

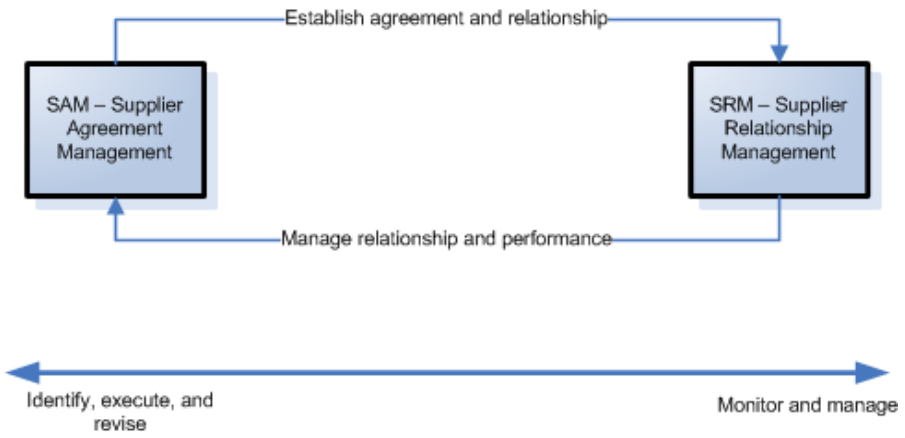


Figure 12: Supplier Management Cluster

Vulnerability, incident, and risk cluster

One of the most important clusters in the CERT Resiliency Engineering Framework is the vulnerability, incident, and risk cluster. An organization can often prevent costly and potentially damaging reaction and response to disruptive events by improving its competencies for detecting events, incidents, vulnerabilities, threats, and risks before they have an opportunity to send the organization into a reactive state. The cluster of competency areas that address proactive identification—VM – Vulnerability Management, RISK – Risk Management, and IMC – Incident Management and Control—are focused on identifying and addressing these potential disruptions and responding in a way that limits or controls not only the organizational impact but also the resources devoted to the response. Included in this cluster is the MON – Monitoring competency area, because it represents the organization's ability to actively look for and know when an anomaly or other unusual data is presented that might indicate a potential event, incident, vulnerability, threat, or risk that the organization must address.

Figure 13 is a simple illustration of the relationship between VM, RISK, IMC, and MON.

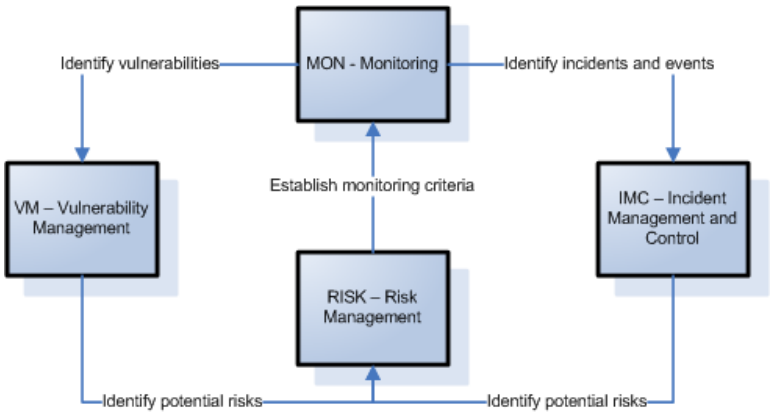


Figure 13: Vulnerability, Incident, and Risk Cluster

[17] SAM and SRM do not codify the competency objectives and practices for end-to-end supply chain management. They are limited to the interaction between suppliers and the organization and the operational resiliency of assets and services for which they share responsibility.

5.8 PROCESS MANAGEMENT

Process Management competencies represent those that are focused on measuring, managing, and improving the resiliency engineering process. These competencies establish the initial application of process improvement concepts to the resiliency engineering process and, by default, to the disciplines of security and business continuity. Competencies in this category are intended to catalyze the organization's view of resiliency as a manageable and improvable process over which it has a significant level of control. Competencies in this area are expected to expand significantly as more process improvement concepts are introduced to the framework.

Process Management competencies can be expressed by two broad categories:

1. *Data collection and logging* addresses the organization's competencies for identifying, collecting, logging, and disseminating information needed to ensure that resiliency engineering processes are performing consistently and within acceptable tolerances.
2. *Process management* addresses the activities the organization performs to use process information to right-track, improve, and optimize resiliency engineering processes.

The body of knowledge for Process Management competencies is included in Appendix D.

5.8.1 Process Management Competencies

The initial Process Management competencies include

Data Collection and Logging

- MON – Monitoring

Process Management

- PM – Process Management
- MA – Measurement and Analysis

5.8.2 Important Process Management Competency Relationships

There is one important relationship cluster focused around the MON – Monitoring competency.

Monitoring cluster

Beyond providing data to feed threat and risk management, the MON – Monitoring competency area is also a source of collecting and logging data that the organization needs for managing operational resiliency and for improving the resiliency engineering process.

The basic activity in Monitoring is data collection and logging. Data can be collected for many reasons, and thus the Monitoring competency area is of potential benefit to many other organizational processes. In the Monitoring competency, the organization is establishing an enterprise view of what needs to be monitored, how often, what data is to be collected, who is to receive the data, and how the data is communicated to stakeholders.

The relationships in the Monitoring cluster are shown in Figure 14.

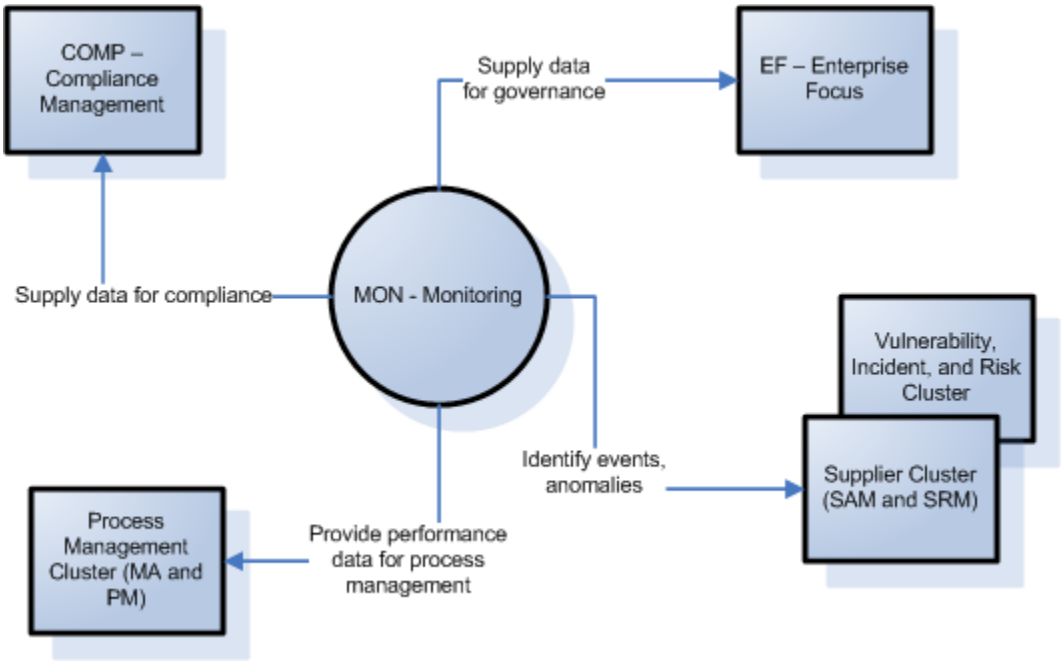


Figure 14: Monitoring Cluster

6 Beginning a Process Improvement Effort

A primary focus of the work presented in this technical report is the development and documentation of a process definition for resiliency engineering. However, a second and equally important objective is the ability to use the process definition as the basis for commencing improvement of an organization's security and sustainability processes.

In this section, model-based process improvement is explored through a discussion of common adoption barriers, dimensions of success, framework entry points, and the consideration of the SEI IDEAL[SM] model for technology transition.

6.1 ADDRESSING BARRIERS TO ADOPTION

Improving basic organizational processes such as hiring and training new personnel or invoicing customers can be a difficult task and can involve the skills and contributions of many diverse areas of the organization. More intricate processes such as the software engineering process are a challenge for process improvement even though they are more clearly bounded. Imagine how difficult the process improvement challenge becomes when the process is enterprise wide in scope, has a diverse set of owners and stakeholders, and is tied directly to the success of meeting the organizational mission. Such is the additional burden of managing and improving the resiliency engineering process.

To be frank, some organizations may not be ready to take on process improvement, particularly at an enterprise level. In addition to requiring strong commitment and sponsorship, it also requires that many layers and levels of the organization adopt a process improvement mindset. Organizations that have been able to achieve enterprise-wide process improvement have noted acculturation as a key success factor.

Besides the need to indoctrinate everyone in the organization to a process improvement view, there are four common barriers that an organization must address and overcome in order to begin process improvement activities and ensure success. These barriers are sponsorship, the organizational structure, the ways in which the process is funded, and in the case of resiliency engineering, the role of information technology in the organization. Each of these barriers is described and addressed below.

6.1.1 Sponsorship and Ownership

One of the most imposing barriers to success for traditional security and business continuity efforts has been sponsorship and ownership. Indeed, the organization and its business units are the beneficiaries of these efforts, yet responsibility for them is generally defined and implemented through technology-focused business units such as information technology (IT). Clearly, this is because there is an assumption in many organizations that security and business continuity are technology-focused activities, and thus leadership and sponsorship for their success is relegated to technology units.

Any change that is worth the organization's time, energy, and resources requires visible and active executive-level sponsorship, regardless of where day-to-day activities are carried out. In particular, for an enterprise-wide process such as operational resiliency (where there are direct effects on strategic objectives), sponsorship is a basic requirement.

[SM] IDEAL is a service mark of Carnegie Mellon University.

The most important aspect of sponsorship is the providing of leadership and support for cultural change. Moving away from a reactive, event-driven approach to resiliency to one that is proactive, comprehensive, and systematic requires executive-led behavior modification. Everyone in the organization must do his or her part, and changing deeply-ingrained behaviors takes constant reminders (in the form of actions and communications) that executive management supports the transition. Where sponsorship is lacking, the organization may never be able to get the necessary changes in attitude, behavior, and actions to take hold. And unfortunately, a failed attempt at process improvement due to a lack of sponsorship may render the organization weaker in the future when it attempts similar efforts.

6.1.2 Organizational Structure

An existing organizational structure can be a severe impediment to process improvement. Organizational structures are devised to efficiently and effectively carry out work, but once established, they are difficult to change or alter because they become part of the organization's culture and personnel become very attached to them. This problem extends to the management of operational resiliency—the way that an organization structures activities such as security and business continuity (particularly if they are done in silos along strict departmental lines) can be an impediment to moving toward an enterprise view of operational resiliency.

In reality, integration of activities and processes at an enterprise level (as established in the resiliency engineering process definition) requires non-traditional organizational structures that do not impede the accomplishment of common goals and objectives. In other words, establishing strict boundaries between collaborative activities such as security and business continuity runs counter to the process definition for resiliency engineering.

6.1.3 Funding Model

Just as organizational structures tend to align across security and business continuity lines, so do the funding models for these activities. Unfortunately, organizations tend to fund resiliency activities at the functional level (i.e., in the security budget) rather than as an enterprise-wide process. When this occurs, there is a disincentive for operational units to collaborate because part or all of their funding must be devoted to activities and personnel who may not be under their direct control and responsibility. Adopting an enterprise view of operational resiliency and a process improvement approach requires that the funding model evolve to one that funds the *processes*, not the operational units. Moreover, compensation for managers of operational units and lines of business should be based on performance measures that support this new enterprise view.

6.1.4 Role of Information Technology

IT traditionally "owns" the functional activities that support operational resiliency. To the extent that this is culturally ingrained, process improvement activities must begin with repositioning and refocusing IT's role. Certainly, IT's stewardship of the resiliency engineering process in itself is not problematic; however, the perception that IT owns and controls the process and that sponsorship of the process improvement effort begins and ends with the chief information officer can be an impediment, particularly for a process that must be adopted by technology and non-technology business units alike. The legacy of security and business continuity's being the domain of IT must be gradually transformed into establishing and nurturing a proper role for IT in the resiliency engineering process definition.

6.2 CONSIDERING PROCESS IMPROVEMENT

Beginning a model-based process improvement approach to any competency seems to be an overwhelming task. But it can be manageable so long as the organization's objectives are kept in perspective. No organization will attempt to adopt and absorb all of the information that has been codified in the process definition for resiliency engineering, nor will it make marked improvements in all processes in a short period of time. Realistically, since the process definition for resiliency engineering is still evolving, it creates a moving target for organizations that choose to begin their efforts immediately.

Getting started on process improvement requires that each organization determine a logical and organizationally relevant starting point. Because each organization has its own unique culture, considerations must be made for how this culture affects the way the organization will approach and adopt the framework. Improving resiliency and operational risk management efficiencies is an appealing goal, but finding operational areas willing to devote resources to such an effort may be a challenge. The key to progress will be starting the process and demonstrating value and success in meeting objectives defined in the implementation strategy.

6.2.1 Dimensions of Process Improvement Success

The software engineering process community has significant experience in transitioning and adopting model-based process improvement approaches. In their book entitled *CMMI Distilled*, the authors state four key process improvement principles that can be universally applied [Ahern 2004]:

1. Maintain executive support.
2. Pick targets carefully.
3. Leverage best practices.
4. Align process improvement with business objectives.

Each of these principles as they apply to the resiliency engineering process is described below.

Maintain executive support

The leaders of the organization are the primary resource for building consensus and support for the process improvement effort. This means that they must not only communicate their support, but they must also act in ways that show their sponsorship through governance, resource allocation and assignment, and employee involvement. They must spearhead the creation of a culture that supports an enterprise-wide process that crosses operational units and traditionally solid organizational lines. Executive support also means that they must be actively *involved* in the process—helping to identify barriers to success, proposing solutions to address these barriers, and being informed when the process improvement effort is bearing fruit.

While resiliency engineering and management at an enterprise level is an emerging discipline, it is likely that one or more c-level executives will emerge as candidates to sponsor and support enterprise-wide process improvement. The emerging importance of the chief risk officer or chief risk manager is an attestation to the increasing importance of risk management as an organization competency, and thus these executives may come to "own" the resiliency engineering space. In addition, the evolving role of the chief information and chief technical officers away from a technology-focused position to one directed at the contribution of information and technology-related assets to achieving strategic objectives continues to be a likely home for commencing process improvement in the resiliency engineering discipline.

Pick targets carefully

Figuring out where to start the improvement process may be the hardest but most important action that an organization takes. Having a reference framework to use as a benchmark is certainly a step in the right direction, but as can be seen by the volume of the resiliency engineering framework outline, such a framework can be intimidating and overwhelming.

It is important for the organization to realize that small improvements go a long way to easing the organization into a process improvement mindset, particularly with disciplines such as security and business continuity that have not previously taken advantage of process improvement concepts. And because these efforts tend to be performed in silos, it may be to the organization's advantage to take on improving competencies that cross these disciplines in order to begin the long road to improving collaboration, communication, and a focus on common organizational goals.

Leverage best practices

Building on what an organization already does is a way to bring people and organizational units into the process improvement effort. They may incorrectly assume that taking on the resiliency engineering process definition, changing their approach to security and business continuity, and improving processes is work that must begin from ground zero. But the organization is actually better served by leveraging best practices already in place.

The resiliency engineering framework makes use of common security and business continuity practices as a foundation for the process definition and the identification of competency objectives and practices. Because it is formed around the practices that many organizations *already use*, an organization may be able to see many entry points into the process improvement framework by examining the practices it currently performs and analyzing how they link to the higher level competency objectives of the framework. Many organizations may be surprised to find how much of the process definition they already cover.

Align process improvement with strategic/business objectives

Strategic planning is the process by which the organization identifies what it needs to achieve and how it is going to achieve it. To be worthy of organizational investment, process improvement efforts must be aligned with and focused on contributing to attaining strategic objectives. Otherwise, why should the organization invest in such activities?

When the process improvement effort is focused on operational resiliency, the connection to strategic objectives is explicit. Improving the way that operational resiliency is managed—making it more predictable and controllable—provides a direct link between the success of process improvement efforts and the organization's ability to achieve strategic objectives. In addition, there is no better way to obtain organizational commitment, involvement, and sponsorship for the process improvement effort than to promote and use it as a means for also improving the achievement of strategic objectives.

6.3 BEGINNING PROCESS IMPROVEMENT

So, where does an organization start to improve the way that it manages operational resiliency? The answer will depend on the organization's level of exposure to process improvement, culture and structure, and a number of other factors.

In this section, a few suggestions for beginning a process improvement effort using the CERT Resiliency Engineering Framework are presented. In reality, because the framework is only presented in outline form in this report, there is not enough detail to make practical use of it. However, organizations that have little

to no experience in large-scale model-based process improvement must begin to consider how they might proceed and what types of approaches might work best. This section is devoted to helping organizations take the first steps.

There are a few ways that an organization can begin to adopt a resiliency engineering mindset and to move toward a process improvement approach. These include

- focusing on adopting and improving specific competencies
- focusing on the resiliency of assets or services
- using an existing perspective such as security and business continuity as a starting point
- adopting a technology transition framework, such as IDEAL, to help to catalyze process improvement

6.3.1 Focusing on Competency Areas

The resiliency engineering framework covers a broad base of specific security and business continuity competencies, as well as a wide array of supporting managerial activities centered on the enterprise and operations. It also ventures into the unexplored territory of process management.

The broad array of competencies represented in the framework means that most organizations will find familiar territory in which to start the process improvement effort. Most organizations have a developed competency in one or more of the competency areas in the framework and thus can begin assessing their current efforts against the framework process definition and identifying areas of strength and possible areas of improvement.

There are, however, a few fundamental areas that should be considered as a starting point[18] for any process improvement effort. These competency areas represent foundational elements of the resiliency engineering process and when mastered can have a profound effect on overall improvement in managing operational resiliency. These competency areas include

- ADM – Asset Definition and Management. Simply being able to identify and manage an inventory of important assets of the organization as they relate to services and the organization's mission is a huge contributor to successfully managing operational resiliency. In addition, the ADM competency area is a higher order competency that directly relates to competencies such as TM – Technology Management; thus mastering ADM creates a foundation for taking on improvement in the competencies represented in the asset cluster. (See Section 5.6.2 for a description and discussion of the asset cluster.)
- RISK – Risk Management. The way in which the organization manages risk directly affects its operational resiliency because it affects how successful it is at exposing and addressing operational risks. The Risk Management competency area is fundamental to ensuring that a risk perspective is a consideration in all of the activities performed in the other framework competencies.
- RRM – Resiliency Requirements Management. Many organizations do not formally create resiliency requirements for their critical assets and services (as represented in RRD – Resiliency Requirements Development), but they do attempt to manage the security and business continuity aspects of the asset from a requirements perspective, if only implicitly. Mastering the Resiliency Requirements Manage-

[18] This does not imply that these competency areas will be the easiest to adopt. Instead, these are competency areas that can have the most direct impact on improving operational resiliency management yet are familiar enough to most organizations to facilitate adoption. The easiest capabilities areas will vary by organization and will be dependent on the maturity of the organization's existing approach to process management and the resiliency engineering process.

ment competency formalizes the use of requirements as the starting point for securing and sustaining these assets and provides a foundation for a requirements-driven resiliency engineering process.

- EF – Enterprise Focus. The importance of sponsorship and oversight for the resiliency engineering process cannot be overstated. As a process that directly supports and aligns with strategic objectives, the organization's efforts in this area will ensure that operational resiliency is a consideration in all of the organization's strategic plans and tactical activities. Catalyzing process improvement efforts by addressing Enterprise Focus is a way to begin the acculturation process that the organization will need to adopt in order to fully adopt a process improvement approach to operational resiliency.

6.3.2 Focusing on the Resiliency of Assets or Services

As described in Section 3, asset resiliency and service resiliency are inextricably tied together—resiliency at both levels translates to operational resiliency at the enterprise level. The choice of whether to address the resiliency engineering framework at the asset level or the services level, however, is strictly an organizational consideration. Some organizations have detailed asset inventories as an outgrowth of higher maturity security processes and therefore are aptly suited to taking on an asset-based approach. Other organizations do not have such granularity as part of their existing security and business continuity activities. Instead, they focus on the business processes and services (often from an application system or technology-specific viewpoint) as they relate and contribute to core strategic and business drivers.

Asset-based approach

An asset-based approach to managing operational resiliency means that the organization focuses its resiliency engineering activities specifically at the asset level and derives service resiliency considerations from this asset view. This approach is suited to organizations that have extensive experience in managing security and business continuity at the asset level and that have well-defined and validated asset inventories that are kept up to date and actively managed as conditions change.

One caution: taking an asset-based approach can be problematic in that the organization may try to include all assets in the scope of resiliency engineering activities, and this may actually make the resiliency engineering process less efficient and effective over time. Assets must be prioritized in consideration of the degree to which they support and sustain critical business process and services.

If an organization chooses to adopt the resiliency engineering framework from an asset perspective, it is imperative that it begin with the ADM – Asset Definition and Management competency area. Its first step should be to take an inventory of organizational assets and then validate and prioritize the list. For the organization to avoid scope issues and to stay focused on productive assets that support core strategic drivers, the assets must be validated for importance based on the services that they support and the value of those services to meeting the organizational mission.

Service-based approach

A service-based approach to managing operational resiliency concentrates on the organization's core services or business processes—those that directly affect and impact the ability of the organization to meet its mission.[19] Performing a service-based approach means that the core important services must be identified and validated against strategic objectives. It also requires that the assets that support those services be identified and associated and that asset resiliency be considered, since service resiliency is derived from

[19] For some organizations, services and business processes are synonymous, and thus a service view is essentially focused at the business process level.

the collective resiliency of the assets that support the service. This approach may help the organization to stay focused on its core strategic drivers much more easily and may help the organization to be more consistent over time.

It is important to note that neither an asset-based nor a service-based approach has yet to be validated as better or more effective than the other; thus, deciding which approach to adopt at this time is purely a matter of organizational preference.

6.3.3 Focusing on Fundamental Resiliency Activities

The CERT Resiliency Engineering Framework is unique in that it defines a process that traverses several core disciplines such as security and business continuity. Naturally, some organizations will want to approach the framework from a vantage point that is familiar and comfortable and for which they have substantial experience and competency. The core disciplines that are most likely to be stepping-off points for starting process improvement for operational resiliency include security, business continuity and disaster recovery, and risk management.

Security perspective

An organization that has a significantly well-developed security plan and program can use it as a platform for adopting the framework. Indeed, there are many competency areas in the framework that have aspects of security management as their foundations, and therefore most organizations will already have expertise in these areas and will be familiar with their intent and objectives.

If an organization chooses to use its security experience as a pathway into the framework, it is suggested that the following competency areas be considered as initial candidates for adoption:

- CM – Controls Management, which addresses security controls for organizational assets
- VM – Vulnerability Management, which focuses on the basic security activity of identifying and addressing technical and physical vulnerabilities
- AMC – Access Management and Control, which deals with the provision of access rights to information and technical assets
- SOM – Security Operations Management, which addresses the fundamental activities necessary to manage security in a technical operations environment
- MON – Monitoring, which provides fundamental information on the state of security controls in the organization

An organization may also want to consider the competency areas included in the asset cluster because each area addresses the unique security considerations of each type of resiliency asset—people, information, technology, and facilities.

In addition, an organization should always consider early adoption of the RISK – Risk Management competency area because risk is a basic consideration in all security activities.

Business continuity perspective

Business continuity activities are clearly important to managing and sustaining the operational resiliency of core organizational services. All organizations perform some degree of business continuity planning, testing, and execution, whether at a technical level (from an application system perspective) or a business-unit level (from a business process or service perspective). Thus, this is generally a core competency for most organizations and is often seen as synonymous with operational resiliency management.

An organization that wishes to catalyze process improvement using its business continuity expertise can find two main entry points to the resiliency engineering framework:

1. SM – Sustainability Management, which represents the range of business continuity activities that an organization performs
2. COMM – Communications Management, which describes aspects of communications that are important to business continuity

In addition, as with the security perspective, an organization may also want to consider the competency areas included in the asset cluster, because each area addresses the unique business continuity and resiliency considerations of each type of resiliency asset.

Business continuity practitioners should consider the RISK – Risk Management competency area concurrently with other suggested competency areas because of the risk considerations that are part of business continuity activities such as business impact analysis.

Risk management perspective

Certainly, if an organization already has a well-developed and executed risk management strategy that extends across the enterprise, this can be a useful advantage in adopting the resiliency engineering framework. Nearly all competency areas in the framework address some aspect of operational risk, and risk considerations (such as tolerance, risk evaluation criteria, etc.) are found throughout the competency objectives and practices of many competency areas. Thus, if an organization chooses to begin process improvement efforts from a risk perspective, the RISK – Risk Management competency area is a recommended initial choice, followed by the other enterprise competency areas (in particular EF – Enterprise Focus, which establishes the organizational targets to which risk considerations are aligned.)

It should be noted that an organization should proceed with caution when relying on one or more of these perspectives to catalyze the process improvement effort. In some cases, instead of encouraging the collaborative and cooperative aspects of the framework, choosing to put the responsibility for improving the resiliency engineering process in the security department or in the hands of business continuity professionals can be interpreted by the organization as placing the accountability and authority in these areas as well. This may be an impediment to process improvement because it can reinforce silos.

6.4 CONSIDERING ADOPTION USING THE IDEAL MODEL

The IDEAL model was originally developed as a companion to CMMI as a way to help organizations to establish and manage a process improvement approach to software engineering. However, the model is useful in helping organizations to adopt other tools, technologies, and methodologies and thus it has since been made applicable to general issues of technology adoption.

The IDEAL model is named for the five phases of adoption that it describes: initiating, diagnosing, establishing, acting, and learning [Gremba 1997]. This is illustrated in Figure 15.

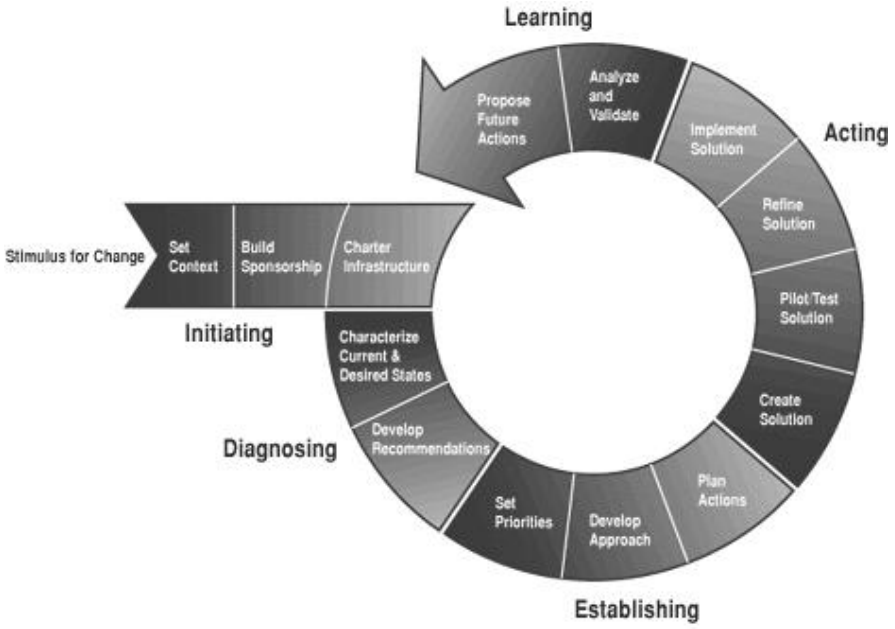


Figure 15: The IDEAL Model for Software Process Improvement

It may be obvious to some that IDEAL is also representative of an expanded Plan-Do-Check-Act cycle (PDCA), often referred to as the "Shewhart cycle" by W. Edwards Demming [Demming 1982], whose quality and improvement theories are pervasive in process improvement models such as CMMI and Six Sigma.

As with any new technology or methodology, ease of adoption is a major factor in getting organizations to make the changes necessary to improve processes. Undoubtedly, this will be a major challenge for the Resiliency Engineering Framework, if only because it traverses the entire enterprise and has no natural organizational owner. And, because the framework fundamentally calls for a change in organizational structures, cultures, and habits that have been cultivated in the security and business continuity communities over a number of years, drastic changes in accepted (yet often flawed) practices and approaches are difficult to make, even if there is a promise of improvement. The IDEAL model is seen as a foundational means for viewing and approaching the process improvement effort that an organization can easily understand, follow, and tailor to its unique operating circumstances.

6.4.1 Stimulus for Change

Simply put, there must be some reason why the organization decides to adopt a resiliency engineering view and to begin a process improvement approach. There can be some obvious reasons (e.g., because other organizations in a specific industry are adopting), but for the most part, there must be some organizational driver and business purpose involved. This is called the stimulus for change, and the first step that an organization must take in adopting a process improvement approach to managing operational resiliency is to determine this catalyst for itself.

For an organization that has experience with process improvement, the stimulus for change might be a desire to extend process improvement concepts and success to areas that previously may not have been considered. For other organizations, the stimulus for change may be the need to control costs, improve return on investment, or support expanding strategic plans. For yet other organizations, a mandate from

stakeholders and executive management might be all that is required to get them moving in the right direction.

Whatever the stimulus, those who will be affected by the changes that process improvement will bring must be able to share the reason for change, support it, and find a way to become involved in it. Otherwise, the cultural change that is needed to support such an undertaking will not be attainable.

6.4.2 Initiating[20]

In addition to establishing the stimulus for change, in the Initiating phase the organization establishes the context for how the change fits its strategic objectives and obtains executive-level sponsorship for the change. As noted previously, there is no more important critical success factor for adopting the resiliency engineering framework than executive-level sponsorship. This is particularly true because operational resiliency is an enterprise concern and no one department or business unit bears the complete responsibility for success. Thus, executive-level sponsorship (and ownership) of the process is essential to obtaining buy-in from disparate parts of the organization and beginning the evolution toward a process-focused approach that transcends operational units. Moreover, sponsorship is an explicit acknowledgement from executive-level management that they intend to assign and support adequate levels of resources to make the process improvement effort a success.

For adopters of the resiliency engineering framework, it is imperative to

- acquaint executive management with the value proposition of resiliency engineering
- demonstrate how a resiliency engineering perspective overcomes the barriers to improving security and business continuity that currently exist
- identify ways in which investment in a process-based approach brings tangible return to the organization and can help the organization to gauge success based on meaningful qualitative and quantitative measures
- show executive management how they can sponsor the cultural change necessary to take on a process approach by
  - keeping resiliency in the forefront of strategic planning and goal setting activities
  - requiring staff to show their contributions to managing operational resiliency as a part of yearly performance management activities
  - putting resiliency topics on the agenda for meetings, symposia, and other gatherings in which the organization considers its performance, plans its growth, and reports its results to stakeholders
  - establishing direct oversight of the organization's operational resiliency as a part of governance

6.4.3 Diagnosing

Diagnosing is the way in which the organization establishes its current state of competency and its desired state and then identifies the gap that exists and needs to be addressed. Akin to performing security assessments and business continuity impact assessments, diagnosis is how the organization comes to reality about the maturity of its current processes and decides how mature they need to be to support the accomplishment of strategic objectives.

Diagnosis is facilitated by having a defined process to use as a benchmark against which measurement will

[20] This section relies heavily on information presented in "The IDEAL Transition Framework – Speeding Managed Change" [Kimbrough 1997].

be taken. The CERT Resiliency Engineering Framework is an initial process definition benchmark that can be used for simple assessment of how well the organization manages operational resiliency and for setting desired performance targets. Based on this diagnosis, the organization can

- analyze why the gap exists and whether it is meaningful
- communicate how the gap affects the organization's ability to manage operational resiliency and to meet security and business continuity goals
- determine what needs to be done to close the gap
- present to executive management the activities that must be performed, the funding required, and most importantly, the benefits that the organization will derive from taking the actions

6.4.4 Establishing

In the Establishing phase, the organization begins the process improvement effort by setting priorities, developing an appropriate approach, and developing action plans. In other words, the organization sets out actively to close the gap in performance by explicitly planning what needs to be done and by prioritizing activities that bring the most value to supporting strategic objectives.

The Establishing activity brings an important new element to security and business continuity because it provides practitioners with a solid foundation for communicating to executive management the rationale for what needs to be performed and why resources should be committed. Instead of requesting funds for vaguely defined and technically focused solutions, the organization can communicate with certainty what actions it intends to take. In addition, because the framework is extensive, the organization can determine where to deploy its limited resources without concern that it is neglecting other important parts of the framework. In other words, a sound and rational basis and plan for proceeding through the framework is established. Such thoughtful planning is frequently lacking in security and business continuity management in organizations today.

6.4.5 Acting

Acting occurs when the organization carries out what it plans to do. Solutions are created, tested, refined, and implemented to close the performance gaps that have been identified (through Diagnosing) and addressed (through Establishing.) In the Acting phase the organization is essentially making improvements that will lead to its target state, whether from an overall operational resiliency management perspective or in a single competency area such as incident management. Acting requires the organization to develop solutions that are functional and sustainable and for which there is long-term executive support. Overall, through the Acting phase, the organization improves the resiliency engineering process based on a systematic and disciplined approach rather than blindly selecting areas to improve or being influenced by the technology of the day.

6.4.6 Learning

Organizations often do not want to turn the mirror on themselves—it is difficult to acknowledge that an effort has been less than successful or that it took more resources and more time than planned. But this type of reality check is important to continuous improvement because it forces the organization to analyze how well it performed and how it can improve its performance in the future.

In the Learning phase, the organization concentrates on analyzing its process improvement experience and determines what works and what does not—in essence, the organization is critiquing its ability to take on a process improvement effort and adopt a process improvement mindset. For example, failure to obtain

proper sponsorship (Initiating) may become an impediment to implementing solutions (Acting) that the organization needs to close performance gaps in one or more framework competencies. Or poorly devised solutions may be found not to produce the results intended because they were not fully analyzed and tested.

Learning provides the organization an opportunity to reflect on the process improvement path it has chosen to take and to make corrections to that path as the process improvement effort continues. It is essential to sustaining improvement in the long term.

6.4.7 Using IDEAL

For those who are just beginning to consider or attempt a process improvement approach to operational resiliency using the CERT Resiliency Engineering Framework, following the IDEAL model provides a disciplined and structured path. It highlights the importance of setting context, gaining sponsorship and support, and providing the structure for change. Using IDEAL gives the organization a systematic way for adopting the framework and built-in gating criteria that the organization can use to determine whether it is succeeding. Not all organizations are equipped to take on a process improvement approach. Using IDEAL gives an organization a way to proceed cautiously so that the effort does not fail and, more importantly, does not preclude future attempts at process improvement.

7 Value Proposition for Financial Institutions

Many of the concepts included in this technical report emanate from the SEI's collaboration with the financial services industry through the Financial Services Technology Consortium (FSTC). FSTC provides financial institutions the ability to come together to discuss technology-related problems and to develop working solutions. In working with the SEI, FSTC members have the ability to perform advanced research on topics such as operational resiliency that are of high priority in their industry.

FSTC first began discussions on the topic of business continuity with an initial focus on benchmarking, strategies for regulatory compliance and resiliency in early 2002. FSTC member institutions were looking for innovations for managing operational risk following a series of wake-up calls that occurred with 9/11, regional power outages, increased cyber attacks, and threats of global terrorism. The FSTC Resiliency Model Project Team formed in late 2004 and began the journey toward the development of a tool to help achieve and manage operational resiliency. The initiative established the following long-term objectives for a resiliency model toolset:

- Help organizations identify the appropriate level of resiliency based on risk tolerance and costs analysis.
- Provide a continuous improvement process to allow organizations to identify, attain, and sustain the appropriate level of resiliency.
- Implement a resiliency-minded culture that helps drive down costs and consistently improves efficiency.
- Provide a benchmark to assess resiliency competencies relative to peers, industry, and third parties.
- Implement common resiliency engineering tools and concepts across all organizations, industries, and geographical boundaries.
- Create ways to measure the resiliency process and determine its efficiency.
- Manage regulatory compliance through a structured process focused on resiliency rather than a reactive, ad hoc process.

7.1 BACKGROUND ON FINANCIAL SECTOR RESILIENCY

The United States financial system processes over three trillion dollars each day or an equivalent of one-fourth the total annual U.S. gross domestic product [FRB 2007]. Thus, financial services companies recognize that they must find better ways to manage risk and optimize the resources being used for business continuity, security, and operations risk management. Financial services is a complex industry, providing fast-paced essential services to virtually every individual and business. The ability to reliably provide credit and liquidity in narrow time frames is a fundamental expectation of all organizations who offer financial services. Business and consumer confidence in the financial services industry's stability and reliability is critical to both the industry itself and to the broader economies that it supports.

It is no surprise that financial service organizations are adept leaders at managing credit, market, and operational risks. Financial services organizations must be careful and flexible risk managers to survive. Historically the focus for risk managers has been primarily in the area of credit and market risk, but today's focus is shifting towards operational risk management. A number of factors, such as industry consolidation, technology advancements, globalization, and terrorism have forced financial organizations to adapt

their risk management practices to meet the escalating threat environment. The financial sector is moving toward a business model that views expenditures on resiliency as necessary investments to remaining competitive in the world marketplace.

For financial services organizations, resiliency can be defined as the ability to deliver financial products and services consistently and reliably in the face of business disruptions. The criteria for quality in the delivery of these products and services now requires more than just reliability; it now includes the goals of privacy and information integrity. Traditional organizational disciplines such as business continuity, information security, and operations have become a strategic focus and management priority. Financial services organizations have elevated these disciplines and are increasingly active in pursuing new innovations in managing operational risks through resiliency.

7.2 FRAMEWORK USE BY FINANCIAL SERVICES ORGANIZATIONS

The motivation to develop the resiliency model was born out of the recognition that the methods being used today by financial services organizations to manage operational risk are inadequate to the task. The value proposition for resiliency engineering is embedded in the concept that what can be measured can be managed. Leveraging the benchmarking and measurement competencies provided by the CERT Resiliency Engineering Framework will be a primary focus of early use activities and associated value statements.

The initial focus by financial services organizations will concentrate on resiliency competency areas that are considered core to business continuity and information security practices, including such areas as sustainability management, access management, and incident management. As organizations gain experience in conducting assessments using familiar competency areas within the Resiliency Engineering Framework, they will expand their scopes to include areas that are less typical risk management components, such as financial resource management, supplier relationship management, and asset definition and management. This approach will allow organizations to build expertise using the Resiliency Engineering Framework and will allow them to continue to refine their approaches and develop comprehensive plans for the expanded implementation of the model. Ongoing efforts to improve the model will be significantly aided through piloting in financial services organizations and the actual utilization of the framework.

8 Future Direction and Research

In this section we describe our future research plans to complete the CERT Resiliency Engineering Framework and the accompanying tools, techniques, and methods that organizations will use to begin their process improvement efforts and to sustain improved processes.

8.1 NEXT STEPS

Our future research and direction is defined by the following activities:

- expanded framework development
- framework assessment
- framework piloting
- community interaction, collaboration, and outreach
- process maturity consideration
- training and awareness

Each of these activities is discussed in more detail below.

8.2 EXPANDED FRAMEWORK DEVELOPMENT

To date, we have developed an outline for the framework that represents the intersection of our fieldwork, research and development, and collaboration with the financial services industry. In essence, it exists as a resiliency engineering body of knowledge. It also represents our best understanding and description of the resiliency engineering process to date. Many individuals have reviewed the scope and contents of the body of knowledge and have provided significant feedback, although additional peer review is needed and welcomed.

But an outline or a body of knowledge is not necessarily usable for beginning or sustaining a process improvement effort. This requires the development of an expanded framework that provides in-depth descriptions of processes, practices, and examples. There are two levels of expanded framework development in our future work: an expanded process definition and the development and addition of subpractices.

8.2.1 Expanded Process Definition

An expanded process definition provides the explanatory material that a process improvement practitioner needs to ensure understanding of the process competency objectives and practices. The expanded process definition provides supporting descriptions of these competency objectives and practices and, most importantly, provides illustrations and examples that can help communicate difficult or unfamiliar terms or concepts. The development of this expanded process definition will also specifically focus on clarifying and standardizing terminology throughout the resiliency engineering concepts and resulting framework. An expanded process definition will be completed and released for all competency areas included in the existing body of knowledge in late 2007.

8.2.2 Development of Subpractices

Subpractices are the way that an organization achieves the specific practices and the competency objectives of a competency area. In other words, subpractices begin to define *how* the descriptive process defi-

nition (the *what*) is accomplished.

In the resiliency engineering process, we are fortunate to have many excellent examples of existing practices in the security, business continuity, and IT operations management disciplines; in fact, it is the existence of these practices that supports our identification and codification of many of the competency areas, competency objectives, and practices that are included in the body of knowledge to date. The broad adoption of these common practices by the community provides a solid foundation for many organizations to enter the framework and begin process improvement efforts.

In the expanded framework, we intend to continue affinity grouping of existing practices with competency areas as necessary; however, more importantly, where practices do not exist to support the competency objectives and practices that have been included in the body of knowledge, we will turn our attention to surveying organizations to determine whether these practices currently exist and to developing practices where necessary.

8.3 FRAMEWORK ASSESSMENT[21]

The ability for an organization to assess its current level of competency using the framework as a benchmark is an essential activity for beginning process improvement efforts. Because to date there has not been a usable process definition for resiliency engineering, assessment instruments in this field are virtually nonexistent. Thus, a major focus of our work is to create initial surveys of practice for each competency area, which organizations can use to diagnose their current levels of competency. In the future, broad use of the surveys and reporting of results may also provide initial benchmarking data.

8.3.1 Develop Surveys of Practice

A survey of practice is a basic tool for assessing an organization's competency in a competency area. A survey of practice is a non-scientific questionnaire that uses the process definition as a basis for asking meaningful questions about how or if an organization performs specific processes. Responses are reflected across a range of criteria that represent increasing levels of competency. The body of knowledge provides the foundation for the surveys; however, as the framework is expanded, the surveys will be updated to reflect improved process descriptions and additional consideration regarding an organization's ongoing ability and commitment to perform processes.

Use of the surveys of practice is envisioned as the initial vehicle for transitioning a process improvement approach to resiliency engineering. Thus, we plan to complete an initial set of surveys (representing all of the competency areas that are included in the existing framework outline) that can be used to help organizations perform basic diagnostic activities during the first half of 2007.

8.3.2 Benchmarking

Benchmarking is the measuring of performance against a standard. One goal of developing an assessment capability for the resiliency engineering framework is to achieve the ability to gather data across a wide range of organizations to validate the framework and to identify gaps, inconsistencies, and omissions. Benchmarking also provides other information that can help an organization make decisions about its process improvement effort relative to other organizations.

Once organizations begin to use the surveys of practice, we intend to actively collect assessment data, ana-

[21] Do not confuse *assessment* with *appraisal*. An appraisal is considered to be an expert-led, independent measure of an organization's process maturity with the framework as the foundation.

lyze it, and provide initial information on the state of practice in resiliency engineering.

8.3.3 SEI-Led Assessment

Using the surveys of practice and the benchmarking data as a foundation, we also plan to develop and deploy an SEI-led assessment methodology and program. This assessment will be conducted by CERT personnel using the expanded resiliency engineering framework and the surveys of practice. Data will be gathered through interviews, document review, and process walkthroughs, and the results of the assessment will be presented to management along with recommendations for proceeding with process improvement activities. An optional workshop will be offered to help organizations to define barriers and enablers to improvement and to identify and prioritize improvement activities. In the future, assessments of process maturity—the ability to repeat and sustain success—will be added.

8.4 FRAMEWORK PILOTING

A major focus of our work in 2007 is the piloting of the expanded resiliency engineering framework. Pilots involve the implementation of the framework and the adoption of competency area practices in an effort to improve the resiliency engineering process. A pilot can include

- diagnosis of current competencies through assessment (as described in Section 8.3.3)
- definition of process improvement targets
- identification of process improvement gaps
- implementation of practices and subpractices to close gaps
- identification and measurement of process improvement results

Pilots not only help an organization to begin the transition to a process improvement approach but also provide much-needed validation and refinement of the framework.

8.5 COMMUNITY INTERACTION, COLLABORATION, AND OUTREACH

8.5.1 Financial Services Technology Consortium

In 2007, we will begin our phase 3 activities with the Financial Services Technology Consortium. These activities include continued collaboration on the development of the expanded framework, the development of the surveys of practice, and the refinement of the resiliency engineering concept and philosophy through active transition and use of the framework.

In 2007, FSTC-sponsored workshops and assessment activities will continue to provide us with a forum from which to draw on the experience and expertise of the financial services community.

8.5.2 User Groups

Utilizing FSTC as an initial organizing entity, a financial industry users group will be formed. This group will provide a venue for financial services organizations to share experiences of the use of the resiliency engineering framework and will also provide an opportunity for the development of any specialized competencies to meet unique needs of financial firms. It is anticipated that the user group interaction will generate extremely valuable dialogue on the application of the model leading to positive insights into the interdependency issues among firms and the development of a stronger final product. Working together, the financial services companies can create a common approach for the use of the resiliency framework that represents the best techniques gained from the experiences of a number of organizations.

Beyond the information sharing and leverage gained through the exchange of ideas, the financial services

user group will also work toward defining and validating an approach that will lead to the successful implementation of the resiliency engineering model. The goals for the implementation strategies and approach will include the development of tools and techniques that ensure the resiliency engineering framework brings value to an organization by providing specific guidance on data collection, analysis, and process improvement.

During 2007, the user group concept will be expanded to include organizations outside financial services to more broadly validate the model and leverage the lessons learned from the ongoing activities and pilot efforts.

8.5.3 Senior Executive Outreach

In 2007, CERT plans to conduct two resiliency engineering workshops aimed at developing the necessary sponsorship and commitment to process improvement at the senior-executive level. These workshops will consist of an interactive session on the concepts of resiliency engineering, the value of a process improvement approach, and an introduction to the framework. A substantial portion of the workshop will be devoted to a user-defined agenda that will be used to identify issues and concerns and to develop workable solutions that will enable sponsorship and transition of the framework.

8.6 EXPLORE PROCESS MATURITY CONSIDERATIONS

The usability of the CERT Resiliency Engineering Framework as a process improvement model will require further exploration and research into the concept of process maturity and the development of a process maturity representation. Initial research indicates that several levels of process maturity can be defined and applied to the existing framework body of knowledge, but additional work is required to transition these concepts for use in process improvement.

The unique subject matter expertise of the SEI in the security and process improvement domains provides a rich source of information and knowledge from which questions and assumptions about process maturity for resiliency engineering can be posed, discussed, and answered. In addition, our efforts to pilot the framework in organizations in the financial sector and beyond will help us to answer questions about process maturity and to determine whether a maturity representation for the framework exists and can be codified.

8.7 DEVELOP TRAINING AND AWARENESS PROGRAMS

Training is a valuable transition tool for promoting new technologies, methods, and tools to a community. With that goal, in 2007 we plan to offer our first course in resiliency engineering based on courses that we have provided to Carnegie Mellon's CIO Institute and other programs. In addition to coursework, we also plan to offer frequent webcasting and podcasting lessons on resiliency engineering on our newly redesigned CERT web portal, www.cert.org.

8.8 OBTAIN COMMUNITY FEEDBACK

In the two years that we have been developing, promoting, and presenting the concepts of resiliency engineering, we have received tremendously useful feedback that is reflected throughout this report and in the resiliency engineering framework outline. Keeping the lines of communication open with the community on this important work is a primary means for sustaining a dialogue that feeds community-driven revisions and improvements to this work. In that spirit, we invite you to provide us with your comments on this report. Your input can be directed to ref-comments@cert.org.

Appendix A CERT Resiliency Engineering Framework: Enterprise Management Competencies

The body of knowledge for the CERT Resiliency Engineering Framework Enterprise Management competencies is described on the following pages.

EF – Enterprise Focus

ENTERPRISE

Purpose

The purpose of Enterprise Focus is to establish sponsorship, strategic planning, and governance over the resiliency engineering process.

Introduction

Managing operational resiliency requires a vast array of skills and competencies. These skills and competencies are spread across the organization and must be focused on common goals and coordinated in execution to achieve and sustain a desired level of resiliency.

Because resiliency is an enterprise concern, the focus and direction for the resiliency engineering process must come from the top: leadership to set direction and ethical standards, sponsorship to provide support and resources, and governance to ensure that the process is achieving its goals as expected. In addition, the resiliency effort must be aligned with and supportive of the achievement of the organization's strategic objectives. Focusing on these objectives provides the rationale for investing in resiliency activities—because they enable the organization to achieve its mission.

The Enterprise Focus competency seeks to ensure that the enterprise owns the resiliency engineering process and provides the necessary level of leadership and governance over the process. The strategic objectives of the organization are explicitly defined as the alignment factor for resiliency plans, programs, and activities. Executive management provides sponsorship to ensure resiliency activities are properly and adequately funded and to promote and nurture a resiliency-aware culture throughout the organization. Finally, the organization's governance activities are expanded to focus directly on resiliency—program objectives are set, standards for acceptable and ethical behavior are established, and the process is monitored to ensure it is achieving its goals. Executive management also provides input and recommendations when the resiliency engineering process is not performing within established standards.

Finally, Enterprise Focus establishes the "critical few" for the organization—the key services that must be resilient to ensure mission achievement. This sets the focus for all operational risk-based activities in the organization. In short, the direction and target for resiliency engineering is established and actions are taken that enable the organization to perform adequately in achieving its targets.

Related Competencies

COMP – Compliance Management
COMP addresses the organization's compliance activities over which EF provides leadership and governance.

MON – Monitoring
MON provides the data and information that the organization needs to provide governance over the resiliency engineering process and resiliency activities.

FRM – Financial Resources Management
FRM ensures the organization considers resiliency as part of the budgeting and resource allocation process.

RISK – Risk Management
Risk Management drives the decisions to focus on the "critical few."

Competency Objectives and Practices

Objective EF-1 Establish Strategic Drivers

The strategic drivers of the organization are established as the foundation for the resiliency engineering process.

Practice EF-1.1 Establish Strategic Objectives

Strategic objectives that support drivers are identified and established as the basis for resiliency activities.

Practice EF-1.2 Establish Critical Success Factors

The critical success factors of the organization are identified and established.

Practice EF-1.3 Establish Organizational Services

The key services that support the accomplishment of strategic objectives are defined and established.

Objective EF-2 Plan Strategically for Resiliency

Strategic planning for the resiliency engineering process is performed.

Practice EF-2.1 Establish Strategic Resiliency Plan

A strategic plan for resiliency is established as the basis for the resiliency engineering process.

Practice EF-2.2 Establish a Resiliency Engineering Program

A program is established to carry out the activities and practices of the strategic resiliency plan.

Objective EF-3 Establish Sponsorship

Visible executive sponsorship for the resiliency engineering process is established.

Practice EF-3.1 Sponsor Funding for Resiliency Activities

A commitment to funding resiliency activities is established at the executive level.

Practice EF-3.2 Promote a Resiliency-Aware Culture

A resiliency-aware culture is promoted through goal setting and achievement.

Practice EF-3.3 Sponsor Resiliency Standards and Policies

The development, implementation, enforcement, and management of standards and policies to establish acceptable and ethical behaviors are sponsored.

Practice EF-3.4 Establish Accountability for Resiliency

Accountability and responsibility for the resiliency engineering process and the achievement of intended outcomes is established.

Objective EF-4 Provide Resiliency Oversight

Governance over the resiliency engineering process is established and performed.

Practice EF-4.1 Establish Resiliency as a Governance Focus Area

Governance activities are focused on the resiliency engineering process and accomplishment of the process goals.

Practice EF-4.2 PERFORM RESILIENCY OVERSIGHT

Oversight is performed over the resiliency engineering process for adherence to established standards, policies, plans, regulations, goals, and objectives.

Practice EF-4.3 ESTABLISH GOVERNANCE METRICS

The data and information required by executive management for establishing and providing ongoing oversight is identified.

Practice EF-4.4 MONITOR AND ESTABLISH CORRECTIVE ACTIONS

Monitoring of the resiliency engineering process is performed and actions are identified to correct deficiencies.

COMP – Compliance Management

ENTERPRISE

Purpose

The purpose of Compliance Management is to ensure awareness of and compliance with an established set of relevant internal and external guidelines, standards, practices, policies, and legislation related to security, privacy, business continuity, and critical infrastructure protection.

Introduction

Regulations, standards, and guidelines are developed and issued by a variety of governmental, regulatory, and industry bodies to enforce (and reinforce) acceptable levels of behavior in areas that are important to the viability and sustainability of organizations and the services they provide to citizens and customers. In particular, the evolving importance of security and resiliency has resulted in a new wave of regulatory bodies and regulations that seek not only to ensure organizational survivability but the survivability of entire industries (such as the banking and finance industry) and to limit undesirable events that have the potential to affect the socio-economic structure of the global economy.

"Compliance" characterizes the activities that the organization performs to identify the regulations to which they are subject and to comply with these regulations in an orderly, timely, and accurate manner. Compliance Management addresses the policies and practices in the organization that support compliance with regulations as an enterprise-wide activity that involves more than just legal and administrative activities.

Compliance with externally directed regulations is the usual focus for organizations, but compliance processes also often address the ability to comply with internally-generated standards and policies such as the organization's information security policy. In addition, compliance is not only important for reinforcing appropriate behaviors; it is also a primary tool in governing the security and resiliency activities in the organization and ensuring they are effectively meeting their goals and objectives.

The Compliance Management competency addresses the organization's ability to establish a compliance plan and program, to identify regulations, standards, and guidelines to which it must comply, and to develop and implement the proper procedures and activities to ensure compliance in a timely and accurate manner. Compliance Management requires the organization to understand its obligations and to collect relevant data in a manner that supports and enables compliance in a way that meets obligations but does not disrupt the organization's focus from its core service delivery.

Related Competencies

EF – Enterprise Focus
EF provides leadership, governance, and oversight over the compliance process.

RRD – Resiliency Requirements Development
Regulations and compliance obligations influence the development of resiliency requirements in RRD.

MON – Monitoring
MON provides some of the data that is needed to satisfy regulatory compliance.

Competency Objectives and Practices

Objective COMP-1 Prepare for Compliance Management

The organizational environment and process for identifying, satisfying, and monitoring compliance obligations is established.

Practice COMP-1.1 Establish a Compliance Management Plan

Planning is performed to develop and implement the organization's process for managing compliance.

Practice COMP-1.2 Identify and Assign Plan Resources

Resources throughout the organization are identified and assigned to compliance-related activities as detailed in the compliance plan.

Practice COMP-1.3 Establish Compliance Guidelines and Standards

The guidelines and standards for satisfying compliance obligations are established and communicated.

Objective COMP-2 Establish Compliance Requirements

The organization's compliance obligations are identified, documented, and communicated.

Practice COMP-2.1 Identify Compliance Requirements

Compliance obligations are identified and documented.

Practice COMP-2.2 Establish Ownership

Owners of compliance obligations are established by identifying the services, business processes, and assets that are affected by the obligations.

Objective COMP-3 Satisfy Compliance Requirements

The organization's compliance obligations are satisfied.

Practice COMP-3.1 Identify Compliance Resources

Resources needed to meet compliance obligations are identified and their responsibilities are communicated and established.

Practice COMP-3.2 Collect and Validate Compliance Data

Data required to meet compliance obligations are collected and validated.

Practice COMP-3.3 Satisfy Compliance Obligations

Compliance obligations are satisfied through compliance activities.

Practice COMP-3.4 Establish Disclosure Process

The satisfaction of compliance obligations is communicated to relevant stakeholders.

Objective COMP-4 Monitor Compliance Activities

The organization's satisfaction of compliance obligations is monitored and adjusted as necessary.

Practice COMP-4.1 Monitor Compliance

Satisfaction of the organization's compliance obligations is independently monitored and deficiencies are identified and addressed.

Practice COMP-4.2 IDENTIFY OPPORTUNITIES FOR IMPROVEMENT

Opportunities for improving the compliance process are continually identified and implemented.

FRM – Financial Resources Management

ENTERPRISE

Purpose

The purpose of Financial Resources Management is to request, receive, manage, and apply financial resources to support resiliency objectives and requirements.

Introduction

Every activity that an organization performs requires a commitment of financial resources. This is particularly true for managing operational resiliency—activities like security and business continuity are resource-intensive and the cost of these activities continues to increase as new threats emerge, technology becomes more pervasive and complex, and the organization shifts its asset base from tangible to intangible assets such as information. Assets require increasingly sophisticated protection strategies and continuity plans which require a financial commitment for their development, implementation, and long-term execution.

Besides ensuring proper funding considerations for resiliency activities, effective consideration of financial resources is also an organizational necessity for managing these activities. The cost of protection and sustainability strategies must be balanced against the value of the potential loss of the productivity of assets and services. In addition, understanding the true cost of providing protection and sustainability of these assets and services is paramount for effectively managing their resiliency. Without relevant information on the costs of protecting and sustaining assets, the organization cannot know when costs are misaligned with asset value and contribution.

Financial Resources Management is focused on improving the organization's ability to apply financial resources to fund resiliency activities while helping the organization to actively manage the cost and return on investment of these activities. The organization establishes a plan for defining financial resources and needs and assigning these resources to resiliency activities. Budgets are established, funding gaps are identified, and costs are tracked and documented. Through effective financial management, the organization establishes its ability to measure return on resiliency investments through calculating "risk vs. reward" and by identifying cost recovery opportunities. In short, Financial Resources Management provides for the possibility that resiliency activities can become investments that the organization uses to move its strategic objectives forward and by doing so recoups its investment through improved value to stakeholders and customers.

Related Competencies

SM – Sustainability Management
Continuity of operations plans developed in SM are funded through the consideration of and application of financial resources as identified in FRM.

CM – Controls Management
FRM provides financial resources in alignment with the selection, implementation, and operation of necessary controls to protect assets and services from intentional or inadvertent harm.

EF – Enterprise Focus
EF sets the strategic direction for financial goals and objectives.

RISK –Risk Management

Risk vs. reward decisions are considered in RISK.

Competency Objectives and Practices

Objective FRM-1 Establish Financial Commitment for Resiliency Activities

The need to consider and assign financial resources to fund resiliency management is established.

Practice FRM-1.1 Determine Financial Responsibilities

Organizational areas that have responsibility for managing and applying financial resources to resiliency management activities are identified.

Practice FRM-1.2 Establish Structure to Support Financial Management

A structure to support the assignment and management of financial resources to resiliency activities is established.

Objective FRM-2 Plan for Financial Resource Allocation

Planning for funding resiliency management activities is performed.

Practice FRM-2.1 Define Funding Needs

Funding needed to support the implementation and management of resiliency requirements and activities is determined.

Practice FRM-2.2 Define Sources of Funds

Sources of funding (capital and expense) to support resiliency management are identified.

Objective FRM-3 Fund Resiliency Activities

The organization's essential activities for managing and sustaining resiliency are funded.

Practice FRM-3.1 Establish Resiliency Budgets

Capital and expense budgets for resiliency management are established.

Practice FRM-3.2 Fund Resiliency Activities

Access to budgeted funds for resiliency management is provided.

Practice FRM-3.3 Fund Off-Budget Resiliency Activities

A method for and access to funds for unplanned and unbudgeted event and incident response is provided.

Practice FRM-3.4 Resolve Funding Gaps

Gaps in funding for resiliency management activities are identified and resolved.

Objective FRM-4 Account for Resiliency Activities

Accounting for the financial commitment to resiliency activities is performed and used for process improvement.

Practice FRM-4.1 Track and Document Costs

Costs associated with resiliency management are tracked and documented.

Practice FRM-4.2 PERFORM COST AND PERFORMANCE ANALYSIS

Cost and performance analyses are performed for funded resiliency management activities.

Objective FRM-5 Measure Return on Resiliency Investments

The return to the organization for investment in resiliency activities is measured and assured.

Practice FRM-5.1 CALCULATE RISK VS. REWARD

Costs of implementing and managing protection and sustainability strategies are actively balanced against the benefits derived from these activities.

Practice FRM-5.2 DETERMINE RETURN ON RESILIENCY INVESTMENT

Return on resiliency investment is calculated.

Practice FRM-5.3 IDENTIFY COST RECOVERY OPPORTUNITIES

Opportunities for the organization to recover costs and investments in resiliency management activities are identified.

RISK – Risk Management

ENTERPRISE

Purpose

The purpose of Risk Management is to identify, analyze, and mitigate risks to organizational assets that could adversely affect the operation and delivery of services.

Introduction

Risk management is a basic and essential organizational competency. The organization must identify, analyze, and mitigate risk commensurate with its risk tolerances and appetite to ensure that it prevents, to the extent possible, disruptions that could interfere with its ability to meet its mission. At a tactical level, to accomplish this goal the organization must control operational risk—the risk that results from the activities that the organization performs on a day-to-day basis. Operational risk is but one type of risk an organization must control; however, it is a pervasive and broadly defined type of risk that is a part of everything the organization does. Simply put, operational risk defines the potential impact that could result from

- failed internal processes
- inadvertent or deliberate actions of people
- problems with systems or technology
- external events

Operational risk is an influencing factor of operational resiliency. The risk of disruption to any asset that supports a business process or service potentially renders the process or service unable to meet is mission, hence reducing its operational resiliency. The organization must identify this risk, analyze it, and determine the extent to which it could affect operations. Mitigating such risk takes a careful balance between protection strategies and sustainability strategies, commensurate with and in consideration of the cost of these strategies and the value of the asset and service to the organization.

The Resiliency Engineering Framework has a significant risk management basis. While it is not a risk management model per se, the framework addresses several aspects of risk management with the objective of contributing to operational resiliency. Thus, risk-management-related activities are pervasive across the entire set of framework competencies that an organization must master to manage the processes for creating operational resiliency.

The Risk Management competency establishes the organization's responsibility to develop and implement an operational risk management plan and program that comprehensively and cooperatively covers the important assets and services of the organization. The organization explicitly establishes its risk tolerances and appetite based on its strategic drivers, market position, competitive environment, financial position, and other factors. Using this appetite as a guide, risks to the assets of the organization are periodically identified, analyzed, and classified, and mitigation strategies are developed and implemented for those risks that the organization cannot afford to ignore. The impact of risk is considered and measured against the organization's risk evaluation criteria. Most importantly, the information gathered in risk assessment is used to improve resiliency processes as the effectiveness of protection and sustainability strategies is assessed and revised as necessary.

Related Competencies

IMC – Incident Management and Control

Potential risks, in the form of events and incidents, are handled in IMC. IMC requires knowledge of the organization's risk criteria to determine when an event or incident requires the organization's attention.

VM – Vulnerability Management

Threats and vulnerabilities that could pose operational risks to the organization are identified in VM and addressed.

RRD – Resiliency Requirements Development

Risk Management has to be requirements driven to meet business objectives. RRD focuses on the alignment between business objectives and resiliency requirements.

EF – Enterprise Focus

Enterprise Focus defines and determines critical business processes and links them to the critical services of the organization.

ADM – Asset Definition and Management

The goal of ADM is to establish the link between services and their important assets.

FRM – Financial Resources Management

FRM is where risk vs. reward calculations are handled based on the risk criteria established in RISK.

Competency Objectives and Practices

Objective RISK-1 Prepare for Risk Management

Preparation for risk management is performed.

Practice RISK-1.1 Determine Risk Sources and Categories

The sources of risk to assets are identified and the categories of risk that are relevant to the organization are determined.

Practice RISK-1.2 Establish a Risk Management Strategy

A strategy for managing operational risk relative to strategic objectives is established and maintained.

Objective RISK-2 Establish Risk Parameters and Focus

Risk tolerances are identified and documented and the focus of risk management activities is established.

Practice RISK-2.1 Define Risk Tolerances

The organization's risk tolerances are defined.

Practice RISK-2.2 Establish Risk Measurement Criteria

Criteria for measuring the organizational impact of realized risk are established.

Objective RISK-3 Identify Risk

Risks are identified through application of risk assessment methodologies.

Practice RISK-3.1 Identify Asset-Level Risk

Risks that affect assets that support services are identified.

Practice RISK-3.2 IDENTIFY SERVICE-LEVEL RISKS

Risks that affect services as a result of asset risk are identified.

Objective RISK-4 Analyze Risk

Risks are analyzed to determine priority and importance.

Practice RISK-4.1 ASSESS RISK

Risks are assessed against risk tolerances and criteria, and the potential impact of risk is characterized.

Practice RISK-4.2 CATEGORIZE AND PRIORITIZE RISK

Risks are categorized and prioritized relative to risk parameters and risks that need to be mitigated are identified.

Practice RISK-4.3 ASSIGN RISK DISPOSITION

The disposition of each identified risk is documented and approved.

Objective RISK-5 Mitigate Risk

Risks to assets and services are mitigated to prevent disruption.

Practice RISK-5.1 DEVELOP RISK MITIGATION PLANS

Risk mitigation plans are developed.

Practice RISK-5.2 IMPLEMENT RISK MITIGATION PLANS

Risk mitigation plans are implemented.

Objective RISK-6 Utilize Risk Information to Manage Resiliency

Information gathered from identifying, analyzing, and mitigating risk is used to improve the resiliency engineering process.

Practice RISK-6.1 REVIEW AND ADJUST PROTECTION STRATEGIES

Controls implemented to protect assets and services from risk are evaluated and updated as required based on risk information.

Practice RISK-6.2 REVIEW AND ADJUST SUSTAINABILITY STRATEGIES

Continuity of operations plans developed to ensure sustainability of services are evaluated and updated as required, based on risk information.

COMM – Communications Management

ENTERPRISE

Purpose

The purpose of Communications Management is to develop, deploy, and manage internal and external communications to support resiliency activities and processes.

Introduction

Communication is a basic organizational activity and competency. From a resiliency perspective, communication is an essential function, tying together disparate parts of the organization which collectively have a vested interest in the sustainability of services before, during, or after a disruptive event. Internally, communications support the development and execution of sustainability plans; externally, communication provides much-needed information to relevant stakeholders on the preparedness of the organization to protect and sustain assets, its capability to handle disruption, and its ability to preserve customer confidence in unsettled times. Most importantly, communications are a critical success factor in the successful execution of continuity of operations plans, particularly during a crisis or disaster.

The Communications Management competency area seeks to capture the communications activities that support and enable operational resiliency. The organization establishes communications requirements commensurate with operational resiliency requirements. Communications guidelines and standards are developed and stakeholders who would benefit from regular information on the organization's resiliency competencies are identified. The communications infrastructure is established and managed to ensure effective and continuous communications flow. The organization also regularly assesses its communications abilities, particularly after an event or crisis, to revise communications requirements and to make improvements in the type and medium of communications and the communications infrastructure.

Related Competencies

IMC – Incident Management and Control
COMM provides standards and guidelines for communicating incidents to relevant stakeholders.

ECFM – Environmental Control and Facilities Management
COMM provides standards and guidelines for communicating with external entities in managing events and incidents.

Competency Objectives and Practices

Objective COMM-1 Establish Communications Requirements and Standards

Resiliency communication requirements and the organizational standards by which these requirements are to be met are established.

Practice COMM-1.1 Identify Relevant Stakeholders

Internal and external stakeholders with whom the organization must communicate relative to resiliency activities are identified.

Practice COMM-1.2 Identify Communication Requirements

The types and extent of communications needed by the organization to support stakeholders are identified.

Practice COMP-1.3 Establish Communications Guidelines and Standards

The enterprise guidelines and standards for satisfying communications needs are established and communicated.

Objective COMM-2 Prepare for Communications Management

The organizational environment and process for developing, deploying, and managing communications is established.

Practice COMM-2.1 Establish a Communications Plan

Planning is performed to develop, deploy, and manage an adequate level of resiliency communications relative to needs.

Practice COMM-2.2 Establish a Communications Program

A program for executing the communications management plan is established and maintained.

Practice COMM-2.3 Identify and Assign Plan Resources

Authority and accountability for carrying out the communications plan and program are assigned to staff.

Practice COMM-2.4 Train Communications Resources

Training is provided to staff to ensure they can adequately fulfill their communication roles as necessary.

Objective COMM-3 Deliver Communications

The activities necessary to deliver communication for resiliency activities on an operational and incident-driven basis are established.

Practice COMM-3.1 Identify Communications Methods and Channels

Communications methods and channels relative to stakeholder and organizational needs are identified and established.

Practice COMM-3.2 Establish Communications Infrastructure

An infrastructure appropriate for meeting the organization's resiliency communication needs is established and managed.

Objective COMM-4 Establish Learning from Communications Management

Pre- and post-incident communications are reviewed to identify and implement improvements in the communications process.

Practice COMM-4.1 Review Incident Communications Activities

The performance of communications plans and programs before, during, and after an incident are reviewed and analyzed.

Practice COMM-4.2 Translate Knowledge into Action

Lessons learned in managing incident communications are utilized to improve communications plans and programs.

OTA – Organizational Training and Awareness

ENTERPRISE

Purpose

The purpose of Organizational Training and Awareness is to provide awareness and training for staff in support of their roles in attaining and sustaining operational resiliency.

Introduction

People are the human capital of the organization. They are an asset that is depended upon for nearly every important organizational business process or service. People are also highly dependent on other organizational assets—they use information, interface with technology, and perform their job responsibilities in facilities. Thus, people are an important component in sustaining the operational resiliency of assets and services; unfortunately, they are also among the hardest assets to manage.

Organizational Training and Awareness is an enterprise competency that seeks to ensure that the organization's human resources are aware of resiliency needs and concerns and that they behave in a manner consistent with the organization's operational resiliency requirements and goals. This requires that they be made aware of the organization's resiliency plans and programs, and that they understand their role in these plans and programs. Staff must also be provided specialized training on a regular basis that establishes resiliency as an organizational competency and encourages improvement in their skill sets relative to their specific or general roles in managing operational resiliency.

In the Organizational Training and Awareness competency the organization establishes and maintains an effective training program and plan to consistently meet the needs of resiliency staff and to close any gaps in skill requirements. In addition, the organization manages the training activities provided for staff by documenting training activities and keeping training records. This documentation provides the organization an ability to review training effectiveness, identify and analyze trends, and make improvements in training and staff acquisition in the future.

Organizational Training and Awareness is a complementary competency to Human Resources Management. Organizational Training and Awareness focuses on general awareness, skill-building, and ongoing training while Human Resources Management is focused on managing the resiliency of the "people" asset.

Related Competencies

HRM – Human Resources Management

The resiliency of the people asset in the organization is established and managed in HRM.

Competency Objectives and Practices

Objective OTA-1 Establish Awareness Program

An awareness program that supports the organization's resiliency program is established.

Practice OTA-1.1 Establish Awareness Needs

The awareness needs of the organization are established and maintained.

Practice OTA-1.2 Establish Awareness Plan

A plan for developing, implementing, and maintaining an awareness program is established and maintained.

Practice OTA-1.3 ESTABLISH AWARENESS CAPABILITY

A capability for delivering awareness programs to staff is established and maintained.

Objective OTA-2 Establish Training Capability

Training capabilities that support the resiliency engineering process are established and maintained.

Practice OTA-2.1 ESTABLISH TRAINING NEEDS

The training needs of the organization are established and maintained.

Practice OTA-2.2 ESTABLISH TRAINING PLAN

A plan for developing, implementing, and maintaining a training program is established and maintained.

Practice OTA-2.3 ESTABLISH TRAINING CAPABILITY

A capability for delivering training to staff is established and maintained.

Objective OTA-3 Conduct Training

Training necessary for staff to perform their roles effectively is provided.

Practice OTA-3.1 DELIVER TRAINING

Training is delivered according to the training plan.

Practice OTA-3.2 ESTABLISH TRAINING RECORDS

Records of delivered training are established and maintained.

Practice OTA-3.3 ASSESS TRAINING EFFECTIVENESS

The effectiveness of the training program is assessed and corrective actions are identified.

Appendix B CERT Resiliency Engineering Framework: Engineering Competencies

The body of knowledge for the CERT Resiliency Engineering Framework Engineering competencies is described on the following pages.

RRD – Resiliency Requirements Development

ENGINEERING

Purpose

The purpose of Resiliency Requirements Development is to identify, document, and analyze the resiliency requirements for services and related assets.

Introduction

Operational resiliency requirements form the foundation for the actions that the organization takes to provide protection and continuity of operations for services. They determine which organizational assets are the most critical to these services and in turn provide the foundation for determining how each service-critical asset needs to be protected and what actions need to be taken to ensure its continuity. More importantly, these requirements establish a common target for risk-based activities such as security, business continuity, and IT operations management. By establishing requirements that reflect the needs of the organization, the protection and sustainability strategies for service-critical assets are focused on common goals. As a result, a shared and committed vision of what needs to be accomplished is created.

Requirements drive engineering-based processes. Thus, in the resiliency engineering process, the Resiliency Requirements Development competency requires the organization to establish resiliency requirements at the enterprise, asset, and service levels. At the asset level, in particular, requirements must be developed to ensure the viability and sustainability of people, information, technology, and facilities—the basic raw materials for organizational business processes and services. Requirements are typically expressed in terms of confidentiality, integrity, and availability because these requirements span the protection (confidentiality and integrity) and sustainability (integrity and availability) activities that the organization performs to ensure resiliency.

Requirement	Asset			
	People	Information	Technology	Facilities
Confidentiality	--	✓	--	--
Integrity	--	✓	✓	✓
Availability	✓	✓	✓	✓

These requirements are analyzed and validated against the organization's strategic drivers to ensure that they reflect the value of assets and services and their contributions to the organization's mission. Deficiencies in requirements are identified and resolved so that the basis for developing and implementing protection and sustainability strategies is sound.

Related Competencies

RRM – Resiliency Requirements Management

Requirements developed in RRD are managed through their life cycle in RRM.

RISK – Risk Management
Resiliency requirements are validated in RISK.

AMC – Access Management and Control
Access to assets is based on resiliency requirements and established and managed in AMC.

Competency Objectives and Practices

Objective RRD-1 Establish Enterprise Requirements and Constraints

The organization's drivers are collected and established as the foundation for resiliency requirements.

Practice RRD-1.1 Establish Enterprise-Level Requirements

The resiliency requirements of the enterprise are established.

Objective RRD-2 Establish Service-Level Requirements

The resiliency requirements for services are developed and established from asset-level requirements.

Practice RRD-2.1 Establish Asset-Level Requirements

The resiliency requirements of assets as they relate to the services they support are established.

Practice RRD-2.2 Assign Enterprise-Level Requirements to Services

Enterprise requirements that affect services are assigned to the services.

Objective RRD-3 Analyze and Validate Service-Level Requirements

The service-level requirements are analyzed and validated.

Practice RRD-3.1 Analyze Requirements

The requirements for services are analyzed to ensure an appropriate level of resiliency.

Practice RRD-3.2 Validate Requirements

The service-level requirements are validated to ensure they adequately reflect enterprise and asset-level requirements.

Practice RRD-3.3 Identify and Resolve Requirements Conflict

Conflicts in requirements due to sharing of assets across services are identified and resolved.

RRM – Resiliency Requirements Management

ENGINEERING

Purpose

The purpose of Resiliency Requirements Management is to manage the resiliency requirements of services and to identify inconsistencies between these requirements and the activities the organization performs to meet the requirements.

Introduction

In conjunction with the Resiliency Requirements Development competency area, the Resiliency Requirements Management competency area seeks to define the life cycle of resiliency requirements—from inception and development to application, monitoring and measurement, and change management. In reality, resiliency requirements constantly evolve as the organization encounters changes in strategic direction, operational complexity, and risk environments. Unfortunately, requirements often are not revisited to ensure alignment with protection and sustainability strategies for service-critical assets, potentially affecting the resiliency of services and the organization's mission. Thus, the organization must make a commitment to and implement dedicated processes that aim to constantly monitor and adjust requirements as these triggers for change are encountered.

Related Competencies

RRD – Resiliency Requirements Development

Requirements are developed in RRD and are managed through their life cycle in RRM.

Competency Objectives and Practices

Objective RRM-1 Manage Requirements

Resiliency requirements are actively managed and inconsistencies between requirements and activities necessary to satisfy them are identified.

Practice RRM-1.1 Obtain an Understanding of Requirements

An understanding of the requirements is obtained from providers to ensure consistency and accuracy.

Practice RRM-1.2 Obtain Commitment to Requirements

Commitments to the requirements are obtained from those who are responsible for satisfying the requirements.

Practice RRM-1.3 Manage Changes to Requirements

Changes to requirements are managed as conditions dictate.

Practice RRM-1.4 Maintain Traceability of Requirements

Bi-directional traceability of requirements between owners and custodians is established.

Practice RRM-1.5 Identify Inconsistencies between Requirements and Activities

Inconsistencies between requirements and the activities performed to satisfy the requirements are identified and managed.

ADM – Asset Definition and Management

ENGINEERING

Purpose

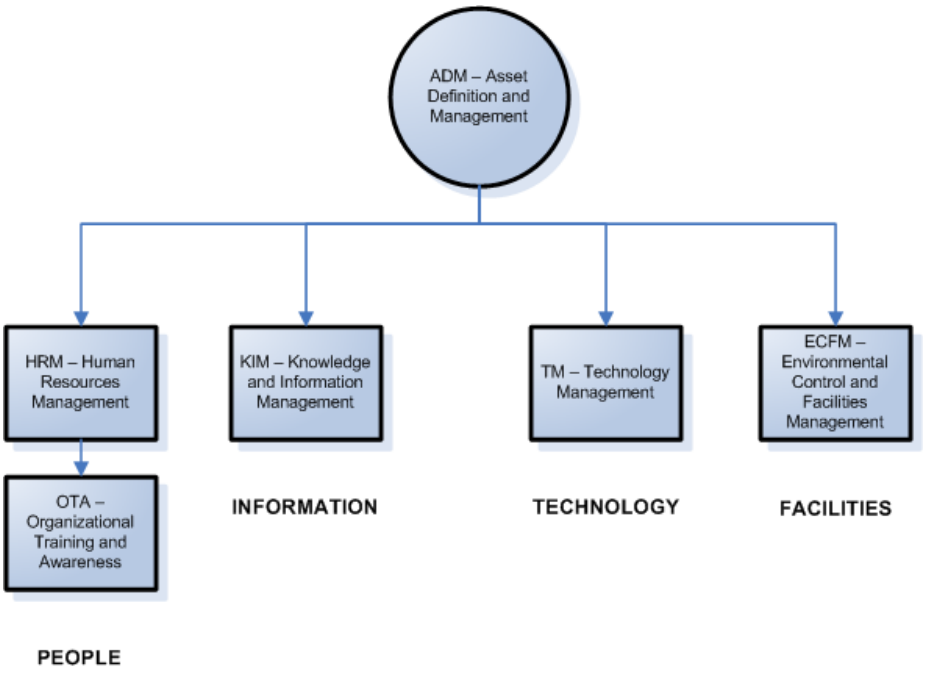
The purpose of Asset Definition and Management is to identify, define, document, and manage organizational assets during their lifecycle to ensure sustained contribution to support organizational services.

Introduction

Mission success for an organization relies on the success of organizational services in achieving their mission. In turn, mission assurance for services depends on the availability, productivity, and ultimately the resiliency, of supporting assets that the service relies upon—*people* to perform and monitor the service, *information* to fuel the service, *technology* to support the automation of the service delivery, and *facilities* in which to operate the service. Whenever any of these assets is affected by disruptive events, the assurance of the mission is less certain and predictable. An organization must be able to identify these service-critical assets, document them, and establish their value in order to develop protection and sustainability strategies commensurate with their value to service delivery.

The Asset Definition and Management competency seeks to establish organizational assets as the focus of the resiliency engineering process. Important organizational assets are identified and profiled (establishing ownership, a common definition, and value), and the relationship between the assets and the organizational services they support is established. The organization also defines and manages the process for keeping the asset inventory current and ensures that changes to the inventory do not result in gaps in protection and sustainability strategies.

The Asset Definition and Management competency is a higher-order competency that establishes the inventory of important organizational assets. The resiliency aspects of these assets (and their related services) are addressed in asset-specific competencies as illustrated below.



Related Competencies

KIM – Knowledge and Information Management
The resiliency of the "information" asset is established and managed in KIM.

TM – Technology Management
The resiliency of the "technology" asset is established and managed in TM.

ECFM – Environmental Control and Facilities Management
The resiliency of the "facility" asset is established and managed in ECFM.

HRM – Human Resources Management and OTA – Organizational Training and Awareness
The resiliency of the "people" asset is established and managed in HRM and OTA.

RRD – Resiliency Requirements Development
Protection and sustainability requirements are developed in RRD.

Competency Objectives and Practices

Objective ADM-1 Establish Organizational Assets

Organizational assets (people, information, technology, and facilities) are identified and the authority and responsibility for these assets is established.

Practice ADM-1.1 Inventory Assets

Organizational assets are identified and inventoried.

Practice ADM-1.2 Establish a Common Understanding

A common and consistent definition of assets is established and communicated.

Practice ADM-1.3 Establish Ownership and Custodianship

The ownership and custodianship of assets is established.

Objective ADM-2 Establish Relationship Between Assets and Services

The relationship between assets and the services they support is established and examined.

Practice ADM-2.1 Associate Assets with Services

Assets are associated with the service or services they support.

Practice ADM-2.2 Analyze Asset-Service Dependencies

Instances where assets support more than one organizational service are identified and analyzed.

Objective ADM-3 Manage Organizational Assets

The life cycle of organizational assets is managed.

Practice ADM-3.1 Identify Change Criteria

The criteria that would indicate changes in an organizational asset or its association with a service are identified and established.

Practice ADM-3.2 Maintain Changes To Assets

Changes to organizational assets are managed as conditions dictate.

SM – Sustainability Management

ENGINEERING

Purpose

The purpose of Sustainability Management is to ensure the continuity of essential operations of services and related assets in the event of an incident or disaster.

Introduction

The continuity of an organization's service delivery is a paramount concern in the organization's operational resiliency activities. The organization can invest considerable time and resources in attempting to prevent disruptive events, but no organization can mitigate all risk. As a result, the organization must be prepared to deal with the consequences of a disruption to its operations at any time. Significant disruption can result in dire circumstances for the organization, including bankruptcy or termination.

Sustainability Management describes the organizational processes involved in developing, deploying, and managing plans for responding to and recovering from events and restoring operations to business as usual. This requires that the organization have a plan and program for sustainability, assign adequate and sufficient resources to these plans and programs, and have the requisite infrastructure to carry out these plans and programs. Based on risk appetite and tolerance, the organization must determine which continuity of operations plans it needs to establish, develop the plans, and test them on a regular and sufficient basis to ensure they remain viable as long as the service is vital to the organization. The organization also must consider the range of continuity activities. Business continuity or contingency plans are developed and implemented to sustain an important service while recovery and restoration plans are focused on bringing services back to an acceptable level of business as usual. To ensure that all plans can be executed at will when called upon, the organization must also develop sufficient logistics and delivery capabilities.

In managing operational risk and resiliency, Sustainability Management is complementary to Controls Management. Controls Management focuses on "condition management" to prevent risk, while Sustainability Management directs the organization's attention to "consequence management" or planning for managing the consequences of risks that are realized. Together, these competencies provide a comprehensive, coordinated, balanced, and holistic approach to managing asset and service resiliency.

Related Competencies

CM – Controls Management
Controls Management focuses on managing threats, vulnerabilities, and risks and is complementary to Sustainability Management.

FRM – Financial Resources Management
Resiliency activities related to continuity of operations are planned, budgeted, and funded in FRM.

RISK – Risk Management
The parameters which influence the development of continuity of operations plans are established in RISK.

IMC – Incident Management and Control
Information on events and incidents and the organization's response to them as defined in IMC influence the development and revision of continuity of operations plans.

Competency Objectives and Practices

Objective SM-1 Prepare for Sustainability Management

The organizational processes for sustainability planning and execution are established.

Practice SM-1.1 Plan for Sustainability Management

Planning for the sustainability management process is performed.

Practice SM-1.2 Establish a Sustainability Management Program

A program for sustainability management is established and maintained.

Practice SM-1.3 Identify and Assign Program Resources

Resources throughout the organization are identified and assigned to sustainability management activities.

Practice SM-1.4 Establish Standards and Guidelines for Continuity of Operations Planning

The guidelines and standards for developing and implementing continuity of operations plans are established.

Objective SM-2 Develop Continuity of Operations Plans

Continuity of operations plans for essential organizational services are developed.

Practice SM-2.1 Identify Plans to be Developed

The continuity of operations plans that must be developed, tested, and executed are identified.

Practice SM-2.2 Develop and Document Plans

The required continuity of operations plans are developed and documented.

Practice SM-2.3 Resource and Train for Plans

Resources are assigned to the required continuity of operations plans.

Practice SM-2.4 Address Plan Logistics

The logistical activities necessary to ensure the ability to execute plans are identified and addressed.

Practice SM-2.5 Archive Plans

Continuity of operations plans are stored and made accessible to those who have a need.

Objective SM-3 Validate Plans

Continuity of operations plans are validated to ensure they address resiliency requirements.

Practice SM-3.1 Validate Plans against Requirements and Standards

Plans are examined to ensure they support resiliency requirements and adhere to the organization's standards and guidelines for plan development.

Practice SM-3.2 Validate Plans against Protection Strategies

Plans are examined to ensure they are in balance to controls implemented to protect assets and services from risk.

Practice SM-3.3 RESOLVE PLAN CONFLICTS

Conflicts between continuity of operations plans are identified and resolved.

Practice SM-3.4 MAINTAIN VIABILITY OF PLANS

The viability and usability of continuity of operations plans is verified periodically.

Objective SM-4 Communicate Plans

The organization's continuity of operations plans are communicated to relevant stakeholders.

Practice SM-4.1 DISTRIBUTE PLANS TO RELEVANT STAKEHOLDERS

Plans are distributed and communicated to relevant stakeholders.

Objective SM-5 Exercise Plans

Continuity of operations plans are exercised to ensure they meet resiliency requirements in execution.

Practice SM-5.1 DEVELOP TESTING PROGRAM AND STANDARDS

A program and standards for plan testing is established and implemented.

Practice SM-5.2 ESTABLISH EXERCISE OBJECTIVES

The objectives of the plan exercise are identified and documented.

Practice SM-5.3 EXERCISE PLANS

Plans are exercised and monitored on a regular basis and results are collected and documented.

Practice SM-5.4 IDENTIFY GAPS AND OPPORTUNITIES FOR IMPROVEMENT

Opportunities for improving continuity of operations plans are identified and implemented.

Objective SM-6 Execute Plans

Continuity of operations plans are executed and post-execution review is established and performed.

Practice SM-6.1 EXECUTE PLANS

Continuity of operations plans are executed.

Practice SM-6.2 PERFORM POST-EXECUTION REVIEW

Post-execution review is performed to identify plan shortfalls and to improve control selection and implementation.

Objective SM-7 Manage Plan Changes

Changes to continuity of operations plans are identified and managed.

Practice SM-7.1 ESTABLISH CHANGE CRITERIA

Change criteria for continuity of operations plans is established.

Practice SM-7.2 MAINTAIN CHANGES TO PLANS

Changes are made to continuity of operations plans as conditions dictate.

CM – Controls Management

ENGINEERING

Purpose

The purpose of Controls Management is to identify, implement, and manage a control structure that protects the essential operations of assets, business processes, and services from intentional or inadvertent misuse, disruption, or harm.

Introduction

Controls are the methods, policies, and procedures—manual or automated—that are adopted by an organization to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, the promotion of administrative efficiency, and adherence to standards. From an operational standpoint, controls are established to ensure the continued, effective operation of services to meet their missions.

Controls are implemented as an extension of the protection strategies for organizational assets and services. Implementing controls that protect assets from intentional or inadvertent harm enhances the resiliency of services that use those assets. A layering of administrative, technical, and physical controls provides a wide range of protection for all types of tangible and intangible assets. The Controls Management competency area addresses the need to set control objectives and establish an appropriate level of controls. It also requires the organization to identify control gaps that could expose assets to vulnerabilities and risks and to manage changes in the control structure commensurate with the redeployment of assets as organizational conditions dictate.

Controls Management is complementary to Sustainability Management. Together, Controls Management and Sustainability Management address the condition and consequence aspects of the risk equation and provide a balanced and holistic approach to managing asset and service resiliency.

Related Competencies

SM – Sustainability Management
The strategies for managing the consequence of realized risk are developed in SM.

MON – Monitoring
Control effectiveness is monitored in MON.

COMP – Compliance Management
Controls for compliance purposes are selected in COMP and managed in CM.

Competency Objectives and Practices

Objective CM-1 Establish Control Objectives

The control objectives that support the organization's resiliency requirements are established.

Practice CM-1.1 Define Control Objectives

Control objectives that represent resiliency requirements are established as the basis for selection, implementation, and management of the organization's control structure.

Objective CM-2 Establish Resiliency Controls

Resiliency controls that support control objectives are established.

Practice CM-2.1 Establish Enterprise-Level Resiliency Controls

Enterprise-level controls that universally apply to services and assets are identified and established.

Practice CM-2.2 Establish Service-Level Resiliency Controls

Controls that protect services from disruption are identified and established.

Objective CM-3 Analyze and Validate Controls

Controls are analyzed and validated to ensure they support the achievement of control objectives.

Practice CM-3.1 Analyze and Validate Controls

Controls are analyzed for appropriateness in achieving control objectives.

Practice CM-3.2 Identify Control Gaps

Inconsistencies between control objectives and the control structure in place are identified and remedied.

Practice CM-3.3 Report Control Weaknesses to Management

Weaknesses in the control structure are reported to management for action.

Objective CM-4 Manage Control Changes

Changes to control objectives and the control structure are managed as conditions dictate.

Practice CM-4.1 Manage Changes to Control Objectives

Changes to control objectives are managed as resiliency requirements change.

Practice CM-4.2 Manage Control Changes

Changes in the control structure are implemented as control objectives change.

Appendix C CERT Resiliency Engineering Framework: Operations Competencies

The body of knowledge for the CERT Resiliency Engineering Framework Operations competencies is described on the following pages.

SAM – Supplier Agreement Management

OPERATIONS

Purpose

The purpose of Supplier Agreement Management is to manage the ongoing acquisition of products and services from suppliers for which there exists a formal agreement.

Introduction

Suppliers are business partners that play an integral part in an organization's day-to-day execution of services and business processes. Suppliers are necessary because few organizations have (or can afford to have) core competencies in all of the tasks they must perform. Thus, organizations source necessary products and services from suppliers to supplement their capabilities.

Unfortunately, the use of suppliers presents potentially increased levels of risk for organizations in managing end-to-end resiliency of business processes and services. When the execution of a business process extends outside of the organization's control, there is less ability to affect or predict mission assurance, in part because mission assurance is dependent on the resiliency of the supplier.

The Supplier Agreement Management competency describes the fundamental activities that the organization performs to establish suppliers, develop and implement agreements with suppliers, and manage supplier agreements over the life of the supplier relationship. To establish collaborative responsibility and management of resiliency with suppliers, the organization must first select suppliers based on their capability and capacity to provide resilient products and services and to protect and sustain organizational assets when they are in the supplier's custodial care. The organization must have criteria for selecting suppliers that reflect its risk tolerances and resiliency requirements. Once suppliers are established, the organization must actively manage the relationship with the supplier to ensure end-to-end resiliency of business processes as conditions and risk environments change.

The Supplier Agreement Management competency area establishes suppliers and agreements with suppliers, while the *Suppler Relationship Management* competency seeks to perform active management of the ongoing relationship.

Related Competencies

SRM – Supplier Relationship Management
Active management of the ongoing relationship with suppliers is performed in SRM.

RISK – Risk Management
Criteria for selecting suppliers based on risk are established in RISK.

CM – Controls Management
Controls with which the supplier must conform are identified and managed in CM.

RRD – Resiliency Requirements Development
The requirements established in RRD must be communicated to and included in agreements with suppliers.

Competency Objectives and Practices

Objective SAM-1 Establish Supplier Agreements

Agreements with suppliers are established and managed.

Practice SAM-1.1 DETERMINE PRODUCTS AND SERVICES TO BE ACQUIRED

The products and services that are to be acquired to support the organization are determined.

Practice SAM-1.2 SELECT SUPPLIERS

Suppliers are selected based on an evaluation of their ability to meet needs and resiliency requirements.

Practice SAM-1.3 ESTABLISH SUPPLIER AGREEMENTS

Formal agreements with the suppliers are established and maintained.

Objective SAM-2 Execute Supplier Agreements

Agreements with suppliers are satisfied by the supplier and the organization.

Practice SAM-2.1 EXECUTE THE SUPPLIER AGREEMENTS

Activities with the supplier as specified in the supplier agreement are performed.

Objective SAM-3 Manage Supplier Agreements

Agreements with suppliers are satisfied by the supplier and the organization.

Practice SAM-3.1 INVENTORY AGREEMENTS

Existing supplier agreements are identified and inventoried.

Practice SAM-3.2 ANALYZE AGREEMENTS

Agreements with suppliers are analyzed to identify interdependencies and resolve potential conflicts.

Practice SAM-3.3 MAINTAIN AND REVISE AGREEMENTS

Agreements are maintained and revised as necessary to reflect current resiliency requirements.

SRM – Supplier Relationship Management

OPERATIONS

Purpose

The purpose of Supplier Relationship Management is to identify and manage resilient relationships with suppliers to ensure end-to-end operational resiliency for services.

Introduction

A viable and productive relationship with suppliers is paramount to ensuring the end-to-end resiliency of business processes for which suppliers provide important products and services. For this reason, the organization must manage the relationship to ensure that it continues to meet requirements throughout its existence and while operating and risk environments continue to evolve.

The competency objectives and practices of Supplier Relationship Management are complementary to the Supplier Agreement Management competency area. In Supplier Agreement Management, the organization establishes the products and services that it requires, selects appropriate suppliers, establishes agreements with the suppliers, executes the agreements, and manages the agreements for the duration of the relationship with the supplier. In contrast, in the Supplier Relationship Management competency area, the organization seeks to establish the performance management criteria for the relationship, measure the performance, and manage any changes in the relationship that might warrant re-visiting and revising the agreement. Across these two competency areas the life cycle of the organization-supplier arrangement and relationship is established, managed, and when necessary, terminated.

Related Competencies

SAM – Supplier Agreement Management
Managing agreements with suppliers is performed in SAM.

Competency Objectives and Practices

Objective SRM-1 Establish Supplier Performance Criteria

The performance criteria for suppliers are established.

Practice SRM-1.1 Establish Enterprise Criteria

Enterprise-wide performance criteria that affect all supplier agreements are established.

Practice SRM-1.2 Establish Resiliency Performance Criteria

The terms of the agreements with suppliers (with respect to operational resiliency) are established and documented.

Objective SRM-2 Monitor Supplier Performance

The performance criteria for suppliers are established.

Practice SRM-2.1 Monitor and Manage Supplier Performance

The performance of suppliers is monitored and appropriate corrective actions are taken where necessary.

Objective SRM-3 Manage Relationship Changes

Changes in suppliers and supplier relationships that could affect resiliency are identified and managed.

Practice SRM-3.1 IDENTIFY SUPPLIER CHANGES

Changes to suppliers are identified.

Practice SRM-3.2 MANAGE CHANGES TO SUPPLIER RELATIONSHIPS

Changes in the nature of existing relationships with suppliers are identified and managed.

VM – Vulnerability Management

OPERATIONS

Purpose

The purpose of Vulnerability Management is to identify, analyze, and manage organizational vulnerabilities.

Introduction

Vulnerabilities are potential disruptions to assets that can affect the viability of services that the assets support. They can be weaknesses in the physical or technical infrastructure of the organization or flaws or defects in technology and information. All assets of the organization that are operationally deployed—people, technology, information, and facilities—are subject to some level and type of vulnerability.

If exploited, vulnerabilities may become risks to the organization that can impact the organization in negative ways. However, vulnerability management is not risk management; instead, vulnerability management is an essential process that focuses on the threat environment and provides valuable insight into potential risks that must be managed in the risk management process. Identifying and understanding these threats and determining their potential for impacting the organization is essential to, and greatly enhances, the overall risk management capabilities of the organization.

The Vulnerability Management competency describes the organization's ability to establish a vulnerability management plan and program and to assign enterprise-wide resources to carry out the plan and program. The organization identifies and analyzes vulnerabilities—physical, technical, human, and organizational—across the enterprise and communicates relative information about these vulnerabilities to other organizational processes that require this information. Strategies are developed to reduce the organization's exposure to vulnerabilities or to lessen the likelihood that vulnerabilities can be exploited by threat actors. In this way, the organization is essentially also mitigating risk where the exploited vulnerability has the potential to impact the organization.

Vulnerability Management also provides the organization an important opportunity to improve processes that may lead to exposures and vulnerabilities. Vulnerabilities are logged and tracked, and root-cause analysis and trending is performed on them to determine if breakdowns in other organizational processes are resulting in exposure. This knowledge is translated into improved protection strategies, updated sustainability strategies, and improvements in the processes.

Related Competencies

CM – Controls Management
Controls are established and implemented in CM to address known vulnerabilities.

IMC – Incident Management and Control
Events and incidents identified in IMC are vulnerabilities that require organization attention.

RISK – Risk Management
Risks that result from the identification of vulnerabilities are addressed in RISK.

MON - Monitoring
Monitoring performed in MON is focused on assisting in the identification of technical and physical vulnerabilities.

OTA – Organizational Training and Awareness
Awareness training is performed in OTA to increase resiliency awareness and reduce human vulnerabilities.

ECFM – Environmental Control and Facilities Management
Geographical vulnerabilities are addressed in ECFM.

HRM – Human Resources Management
Reducing vulnerability exposure for staff is addressed in HRM.

SOM – Security Operations Management
Vulnerability management activities are carried out in SOM.

COMM – Communications Management
Vulnerabilities are communicated to relevant stakeholders through processes established and managed in COMM.

Competency Objectives and Practices

Objective VM-1 Establish Vulnerability Management Process

The process for identifying, analyzing, and managing organizational vulnerabilities is established and maintained.

Practice VM-1.1 Establish a Vulnerability Management Plan

A strategy for organizational vulnerability management is established and maintained.

Practice VM-1.2 Identify and assign Plan Resources

Resources throughout the organization are identified and assigned to vulnerability management activities.

Objective VM-2 Identify and Analyze Vulnerabilities

The process for identifying and analyzing vulnerabilities is established.

Practice VM-2.1 Perform Vulnerability Monitoring

Information about potential vulnerabilities is collected.

Practice VM-2.2 Identify Vulnerabilities

Vulnerabilities are actively discovered through monitoring and other information sources.

Practice VM-2.3 Analyze Vulnerabilities

Vulnerabilities are analyzed to determine if they pose potential risk to the organization.

Practice VM-2.4 Communicate Vulnerability Information

Vulnerability information is communicated to relevant stakeholders.

Objective VM-3 Manage Exposure to Vulnerabilities

Strategies are developed to manage exposure to identified vulnerabilities.

Practice VM-3.1 Reduce Exposure

Vulnerabilities are addressed through implementation of preventative controls and other strategies.

Objective VM-4 Establish Learning from Vulnerability Management

Lessons learned from managing vulnerabilities are transformed into actions that support ongoing operational resiliency.

Practice VM-4.1 Log and Track Vulnerability Handling Activities

Vulnerabilities are logged and tracked from identification to disposition.

Practice VM-4.2 Perform Root-Cause Analysis

Vulnerabilities are reviewed to determine and address underlying causes.

Practice VM-4.3 Translate Knowledge into Action

Lessons learned in vulnerability management are utilized in other related organizational processes

IMC – Incident Management and Control

OPERATIONS

Purpose

The purpose of Incident Management and Control is to establish processes to identify and analyze incidents and to determine an appropriate organizational response.

Introduction

Throughout an organization's operational environment, disruptions occur on a regular basis. They may occur as the result of intentional actions against the organization—such as a denial-of-service attack or the proliferation of a computer virus—or because of actions over which the organization has no control such as a flood or earthquake. Disruptive events can be innocuous and go unnoticed by the organization, or to the contrary, can significantly impact operational capacities that affect the organization's ability to carry out its goals and objectives.

To manage operational resiliency, an organization must become adept at preventing disruptions and ensuring continuity of operations when a disruption occurs. However, not all events can be prevented; thus, the organization must have the capability to identify events that can affect its operations and respond appropriately. This requires the organization to have processes to recognize potential disruptions, analyze them, and determine if, how, and when to respond.

The Incident Management and Control competency focuses the organization's attention on the life cycle of an incident—from detection to analysis to closure. The organization establishes the incident management plan and program and assigns appropriate resources, either in a team setting or across the enterprise. Event reporting capabilities are established and the organization sets criteria to know when events become incidents that demand the organization's attention. The incident life cycle is defined from incident identification through analysis, response, and closure. Support activities such as communication, logging and tracking incidents, and preserving incident evidence are defined and established. Most importantly, the organization performs post-incident review to determine what can be learned from incident management and applied to improved protection and sustainability strategies as well as improvements in the incident management process and life-cycle management.

Related Competencies

RISK – Risk Management
Events and incidents identified in IMC are potential risks that must be analyzed and mitigated in RISK.

MON - Monitoring
Information on potential events and incidents may be collected and communicated in MON.

VM – Vulnerability Management
Vulnerabilities identified in VM are a source of potential event and incident information in IMC.

COMM – Communications Management
Strategies for organizational communications are developed in COMM.

SOM – Security Operations Management
SOM is a source for identification of incidents, forensic data collection, logs, and so forth.

Competency Objectives and Practices

Objective IMC-1 Establish Incident Management and Control Process

The organizational process for identifying, analyzing, responding to, and learning from incidents is established.

Practice IMC-1.1 Plan for Incidents and Response

Planning is performed for developing and implementing the organization's incident management and control processes.

Practice IMC-1.2 Resource Incident Management Plan

Resources are identified and assigned to the incident management plan.

Objective IMC-2 Establish Incident Identification

The processes for identifying events and incidents are established.

Practice IMC-2.1 Establish Event Reporting

Sources of event reporting and the processes from which incidents may be identified are defined.

Practice IMC-2.2 Define and Maintain Incident Criteria

Criteria for identifying incidents is defined and maintained.

Objective IMC-3 Manage Incident Life Cycle

The life cycle of incidents is defined and managed.

Practice IMC-3.1 Establish Communications Plan and Process

A plan for the communication of incidents and a process for managing ongoing communications are established.

Practice IMC-3.2 Establish Escalation Process

The process for escalating incidents to relevant responders and stakeholders is established.

Practice IMC-3.3 Log and Track Incidents

Incidents are logged and tracked from inception to disposition.

Practice IMC-3.4 Collect, Document, and Preserve Incident Evidence

The process for collecting, documenting, and preserving incident evidence is established.

Practice IMC-3.5 Close Incidents

Incidents are closed after relevant actions have been taken by the organization.

Objective IMC-4 Analyze and Respond to Incidents

The process for analyzing and responding to incidents is established.

Practice IMC-4.1 Analyze Incidents

Incidents are analyzed to understand the problem and determine an appropriate response.

Practice IMC-4.2 Respond to Incidents

A response to incidents is enacted to prevent or limit their organizational impact.

Practice IMC-4.3 COMMUNICATE INCIDENTS

Strategies for communicating information about incidents to relevant stakeholders are developed and implemented.

Objective IMC-5 Establish Incident Learning

Lessons learned from identifying, analyzing, and responding to incidents are translated into actions to enhance asset protection and sustainability.

Practice IMC-5.1 PERFORM POST-INCIDENT REVIEW

Post-incident review is performed to determine underlying causes.

Practice IMC-5.2 INTEGRATE WITH PROBLEM MANAGEMENT PROCESSES

A link is established between incident management and the organization's IT problem management process.

Practice IMC-5.3 TRANSLATE EXPERIENCE TO STRATEGY

Lessons learned are analyzed and translated into asset protection and sustainability strategies.

AMC – Access Management and Control

OPERATIONS

Purpose

The purpose of Access Management and Control is to ensure that the user population is established and provided access rights to assets commensurate with the asset's business and resiliency requirements.

Introduction

In order to support business processes, people use assets such as information, technology, and facilities. This requires that people have sufficient access to these assets (commensurate with business requirements and their corresponding job responsibilities) to ensure that services remain productive. The productivity of services also depends on protecting assets from being accessed by people who do not have a legitimate business purpose or job responsibilities. Thus, the protection strategy for a critical organizational asset requires the implementation of controls that provide access to legitimate users and prevent access to those who could intentionally or inadvertently harm the asset. These access controls are a key layer of protection for an asset and form a substantial portion of the organization's protection strategy for assets and services.

The Access Management and Control competency establishes the processes for identifying users and assigning them privileges—both technical/logical and physical—to important organizational assets. The organization establishes the user environment—the pool of users to whom access rights and privileges can be assigned—and manages the user community as access needs evolve and change. Access rights are assigned in accordance with the user's job responsibility and in alignment with the resiliency requirements of the assets and service to which access is being granted. The organization monitors access rights and revises them in a timely manner to ensure they reflect current needs as assets, users, and user roles change.

Related Competencies

RRD – Resiliency Requirements Development
The requirements against which access rights and privileges are substantiated and validated are established in RRD.

SOM – Security Operations Management
The implementation of access rights and privileges is performed in SOM.

ECFM – Environmental Control and Facilities Management
Access rights and privileges specific to facilities are considered in ECFM.

Competency Objectives and Practices

Objective AMC-1 Establish and Control User Environment

The user environment is established and controlled to ensure the satisfaction of business and resiliency requirements for assets.

Practice AMC-1.1 Register and Profile Users

Users of organizational assets are registered and profiled.

Practice AMC-1.2 Establish and Document User Community

The user community is established and documented.

Practice AMC-1.3 MONITOR AND MANAGE CHANGES TO USER COMMUNITY

Monitor for and manage change to the user community.

Practice AMC-1.4 IDENTIFY AND CORRECT INCONSISTENCIES

Inconsistencies between the user inventory and the active user community are identified and resolved.

Objective AMC-2 Manage and Control Access Rights

User access rights to organizational assets are managed and controlled.

Practice AMC-2.1 ASSIGN ACCESS RIGHTS

Appropriate access to organizational assets is assigned based on user roles and responsibilities.

Practice AMC-2.2 MANAGE CHANGES TO USER ACCESS PRIVILEGES

Changes to access rights as assets, users, and user roles change are identified and managed.

Practice AMC-2.3 MONITOR AND RECONCILE ACCESS RIGHTS

Access rights are monitored and inconsistencies are identified and corrected.

ECFM – Environmental Control and Facilities Management

OPERATIONS

Purpose

The purpose of Environmental Control and Facilities Management is to establish and manage an appropriate level of physical, environmental, and geographical controls to support the resilient operation of services in organizational facilities.

Introduction

People, information, and technology objects "live" within a physical facility—people work in offices, information is stored in file rooms or on servers, and technology is housed in specialized facilities such as data centers. When a facility is disrupted, there is often a cascading effect on the operability of these other assets.

As a complicating factor, organizations may not always have direct control over the facilities in which their services and business processes are executed or their assets are located. Facilities may be owned by the organization, but frequently they are acquired or leased from another organization. These arrangements sometimes also mean that the organization's assets are co-located with other organizations in the same facility. This presents challenges not only for facilities management but for ensuring the operational resiliency of services that depend on these facilities to meet their missions.

The Environmental Control and Facilities Management competency is positioned to address the importance of facilities in the operational resiliency of services as well as the unique issues that facility assets inherit because of their geographical location and the environment in which they operate. In this competency, facility assets are prioritized according to their value in supporting critical organizational services. Physical, technical, and administrative controls that keep facility assets viable and sustainable are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, facility risks are identified and mitigated in an attempt to prevent disruption where possible. Because facilities are intricately tied to the geographical location in which they operate, the unique dependencies of the facility on its adjacent environment are identified and actively managed.

Related Competencies

ADM – Asset Definition and Management
Facility assets are identified, defined, and managed in ADM.

AMC – Access Management and Control
The management of users and access rights and privileges is established in AMC.

CM – Controls Management
An enterprise view of controls as the mechanism for asset protection is established in CM.

Competency Objectives and Practices

Objective ECFM-1 Establish and Prioritize Facility Assets

Facility assets are prioritized to ensure the resiliency of key services that they support.

Practice ECFM-1.1 PRIORITIZE FACILITY ASSETS

Facility assets are prioritized relative to their importance in supporting the delivery of key services.

Practice ECFM-1.2 Establish Resiliency-Focused Facility Assets

Facility assets that specifically support the organization's continuity of operations plans for key services are identified and established.

Objective ECFM-2 Protect Facility Assets

The physical security controls for existing facility assets and those that are to be acquired or developed are identified, implemented, monitored, and managed.

Practice ECFM-2.1 Assign Resiliency Requirements to Facility Assets

Resiliency requirements that have been defined are assigned to facility assets.

Practice ECFM-2.2 Establish Physical Security Controls

Physical security controls that are required to meet the established resiliency requirements are identified and implemented.

Practice ECFM-2.3 Monitor Control Effectiveness

Physical security controls are monitored for effectiveness and deficiencies are identified and addressed.

Objective ECFM-3 Manage Facility Asset Risk

Operational and environmental risks to the facility assets are identified and managed.

Practice ECFM-3.1 Perform Facility Asset Risk Assessment

Risks to facility assets are periodically identified and assessed.

Practice ECFM-3.2 Mitigate Facility Risks

Risk mitigation strategies for facility assets are developed and implemented.

Objective ECFM-4 Control Operational Environment

The environment in which facility assets are located and operated is controlled.

Practice ECFM-4.1 Manage Environmental Conditions

Environmental conditions of facility assets are managed.

Practice ECFM-4.2 Manage Dependencies on Public Services

Dependencies on public services for facility assets are identified and managed.

Practice ECFM-4.3 Manage Dependencies on Public Infrastructure

Dependencies on public infrastructure for facility assets are identified and managed.

HRM – Human Resources Management

ENTERPRISE

Purpose

The purpose of Human Resources Management is to establish and manage the contributions of people to support the resilient operation of organizational services.

Introduction

People are an important factor in the organization's ability to produce products and deliver services in the pursuit of strategic objectives. Without people and their skills, many business processes could not operate effectively and the mission of organizational services would be in jeopardy. To make effective use of people in the resiliency engineering process, the organization must be adept at acquiring staff with the right skills and must be competent in keeping these staff trained, viable, and productive.

The Human Resources Management competency is focused on the acquisition and development of staff who are important to the ongoing management of the resiliency engineering process. These staff may comprise employees of the organization or may be acquired through outsourcing or supplier relationships, depending on organizational requirements, core competencies, and costs.

In Human Resources Management, the organization reinforces the connection between people and operational resiliency by specifically establishing acceptable performance behaviors and measuring compliance with these behaviors on a regular basis as part of the performance management cycle. In this way, the organization "inculcates" a resiliency-aware and ready culture that is essential for supporting the resiliency process and the organizational mission.

Human Resources Management also focuses on managing the potential threats that could interfere with or interrupt the performance of people and consequently, the services to which their contributions are important. This requires the organization to consider cross training staff for important job responsibilities and to perform succession planning to ensure a steady stream of effective human resources for important job roles and responsibilities. The impact of staff turnover, particularly in key roles in key services, is also considered and addressed. When disruptions occur, Human Resources Management focuses the organization on preparing staff to accept and perform new roles, however temporary, until a return to business as usual can be accomplished. This can be a challenge because of physiological and physical constraints that the organization may have to identify and address before human resources can effectively be re-introduced to a post-event workplace environment. All of these potential issues must be acknowledged and addressed by the organization in order to ensure sustained productivity of human resources throughout the enterprise.

Human Resources Management is a complementary competency to Organizational Training and Awareness. Organizational Training and Awareness focuses on general awareness, skill building, and ongoing training while Human Resources Management is focused on managing the resiliency of the "people" asset.

Related Competencies

OTA – Organizational Training and Awareness

The training and awareness of staff to meet resiliency requirements, needs, and gaps is established and managed in OTA.

SM – Sustainability Management

The role of people in the sustainability of important organizational services and business processes is ad-

dressed in the development of continuity of operations plans in SM.

COMP – Compliance Management
The compliance of people with resiliency requirements, regulations, standards, and internal policies is addressed in COMP.

Competency Objectives and Practices

Objective HRM-1 Acquire and Retain Staff

Staff are acquired and trained to meet resiliency needs.

Practice HRM-1.1 Establish Baseline Competencies

The staffing and skill needs relative to the resiliency engineering process and the resiliency plan and program are established.

Practice HRM-1.2 Inventory Skills and Identify Gaps

The current skill set for resiliency engineering is inventoried and gaps in necessary skills are identified.

Practice HRM-1.3 Match Staff to Needs

Staff are matched to needs based on skills, experience, and training.

Practice HRM-1.4 Acquire Staff to Meet Needs

Resiliency needs are filled through the acquisition and retention of skilled staff.

Objective HRM-2 Manage Staff Performance

The performance of staff to support the organization's resiliency program is managed.

Practice HRM-2.1 Establish Goals and Objectives

Goals and objectives for achieving and supporting the resiliency program are established as part of the performance management process.

Practice HRM-2.2 Measure and Assess Performance

Performance against goals and objectives is measured and corrective actions are identified and communicated.

Objective HRM-3 Manage Staff Resiliency

The resiliency of staff as a critical part of service delivery is actively managed.

Practice HRM-3.1 Identify and Assess Staff Risk

Staff are adequately cross-trained to ensure continuity of services.

Practice HRM-3.2 Cross-Train Staff

Staff are adequately cross-trained to ensure continuity of services.

Practice HRM-3.3 Perform Succession Planning

Key staffing roles and responsibilities are supported through succession planning.

Practice HRM-3.4 PREPARE FOR REDEPLOYMENT

Staff is trained for redeployment to other roles during a disruptive event or in the execution of a continuity of operations plan.

Practice HRM-3.5 MANAGE IMPACT OF STAFF TURNOVER

Turnover of staff is actively managed to ensure minimal impact on operational resiliency.

Objective HRM-4 Manage Staff Logistics

Support for staff during disruptive events and in their return to business as usual is performed.

Practice HRM-4.1 PLAN TO SUPPORT STAFF DURING DISRUPTIVE EVENT

Plans are developed and implemented to ensure support is provided for staff as they perform their duties during a disruptive event.

Practice HRM-4.2 PLAN FOR RETURN-TO-WORK CONSIDERATIONS

Plans are developed and implemented to address return-to-work issues for staff after a disruptive event.

KIM – Knowledge and Information Management

OPERATIONS

Purpose

The purpose of Knowledge and Information Management is to establish and manage an appropriate level of controls to support the confidentiality, integrity, and availability of the organization's information and intellectual property.

Introduction

The importance of information as an organizational asset continues to grow. In fact, the focus of organizations has increasingly turned to intangible assets such that the ration of tangible assets to intangible assets continues to decrease. This supports the assertion that information is one of the most—if not *the* most—important organizational assets. It is the raw material that is used by and created in business processes. The protection of this intellectual and enterprise capital—to ensure that it is available in the form intended for use in business processes and services—is the focus of the Knowledge and Information Management competency area.

The Knowledge and Information Management competency addresses the importance of information in the operational resiliency of services as well as unique issues specific to information such as confidentiality, sensitivity, and privacy. In this competency, information assets are prioritized according to their value in supporting critical organizational services. Physical, technical, and administrative controls that keep information assets viable and sustainable are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, information asset risks are identified and mitigated in an attempt to prevent disruption where possible. Information is classified as to its organizational sensitivity, and considerations are made for the backup and storage of important information in case of loss or destruction, or to support the execution of continuity of operations plans.

Knowledge management is also performed in this competency: the requirement to identify and document the organizational and intellectual knowledge of staff that is important to the effective operation of the organization's business processes and services. This information asset is often undocumented, has poorly developed security requirements, and lacks adequate protection. It is also often one of the most important information assets in the organization.

Related Competencies

ADM – Asset Definition and Management
Information assets are identified, defined, and managed in ADM.

AMC – Access Management and Control
The management of users and access rights and privileges is established in AMC.

CM – Controls Management
An enterprise view of controls as the mechanism for asset protection is established in CM.

RISK– Risk Management
An enterprise view of risk identification, analysis, and mitigation for potential impact on assets and services is established in RISK.

Competency Objectives and Practices

Objective KIM-1 Establish and Prioritize Information Assets

Information assets are prioritized to ensure resiliency of key services in which they are used.

Practice KIM-1.1 Prioritize Information Assets

Information assets are prioritized relative to their importance in supporting the delivery of key services.

Practice KIM-1.2 Establish Resiliency-Focused Information Assets

Information assets that are required to support the organization's continuity of operations plans for key services are identified and established.

Practice KIM-1.3 Categorize and Classify Information Assets

Information assets that support key services are categorized and classified as to their organizational sensitivity.

Objective KIM-2 Protect Information Assets

Administrative, technical, and physical controls for existing information assets and those to be acquired or developed are identified, implemented, monitored, and managed.

Practice KIM-2.1 Assign Resiliency Requirements To Information Assets

Resiliency requirements that have been defined are assigned to information assets.

Practice KIM-2.2 Establish Controls

Administrative, technical, and physical controls that are required to meet the established resiliency requirements are identified and implemented.

Practice KIM-2.3 Monitor Control Effectiveness

Controls are monitored for effectiveness and deficiencies are identified and addressed.

Objective KIM-3 Manage Information Asset Risk

Operational risks to information assets are identified and managed.

Practice KIM-3.1 Identify and Assess Information Asset Risk

Risks to information assets are periodically identified and assessed.

Practice KIM-3.2 Mitigate Information Asset Risk

Risk mitigation strategies for information assets are developed and implemented.

Objective KIM-4 Manage Information Asset Availability

The availability of information assets to support key services is managed.

Practice KIM-4.1 Perform Information Retention and Back-up

Key information assets are backed up and retained to support services during disruptive events.

Practice KIM-4.2 Perform Knowledge Management

The organizational and intellectual knowledge of staff is identified and documented.

SOM – Security Operations Management

OPERATIONS

Purpose

The purpose of Security Operations Management is to perform the day-to-day security functions necessary to support and sustain an appropriate level of operational resiliency.

Introduction

The scope of this competency area is currently under review. Competency objectives and practices will be developed when this review has been completed.

TM – Technology Management

OPERATIONS

Purpose

The purpose of Technology Management is to establish and manage appropriate controls related to the selection, acquisition, and management of technology assets to support the resilient operations of organizational services.

Introduction

Technology is a pervasive organizational asset. Few organizational services are untouched by some aspect of technology—hardware, software, systems, tools, and infrastructure (such as networks) that support services. Technology assets directly support the automation (and efficiency) of business processes and services. For some organizations, technology is a prominent driver in accomplishing the mission and is considered a strategic element. Technology tends to be pervasive across all functions of the organization and therefore can be a significant contributor to strategic and competitive success.

The Technology Management competency addresses the importance of technology assets in the operational resiliency of services as well as unique issues specific to technology such as integrity and availability management. In this competency area, technology assets are prioritized according to their value in supporting critical organizational services. Physical, technical, and administrative controls that keep technology assets viable and sustainable are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, technology asset risks are identified and mitigated in an attempt to prevent disruption where possible. The integrity of technology assets is addressed through master of basic IT capabilities such as configuration, change, and release management. The availability of technology assets, critical for supporting the resiliency of services, is established and managed by controlling the operational environment in which the assets operate, by performing regular maintenance on these assets, and by limiting the potential effects of interoperability issues. Because technology assets typically extend outside of the physical and logical boundaries of the organization, the organization must address the management of suppliers that provide technology assets or support those assets for the organization.

Related Competencies

ADM – Asset Definition and Management
Technology assets are identified, defined, and managed in ADM.

AMC – Access Management and Control
The management of users and access rights and privileges to technology assets is established in AMC.

CM – Controls Management
An enterprise view of controls as the mechanism for technology asset protection is established in CM.

RISK– Risk Management
An enterprise view of risk identification, analysis, and mitigation for potential impact on technology assets and services is established in RISK.

Competency Objectives and Practices

Objective TM-1 Establish and Prioritize Technology Assets

Technology assets are prioritized to ensure resiliency of key services that they support.

Practice TM-1.1 PRIORITIZE TECHNOLOGY ASSETS

Technology assets are prioritized relative to their importance in supporting the delivery of key services.

Practice TM-1.2 ESTABLISH RESILIENCY-FOCUSED TECHNOLOGY ASSETS

Technology assets that are required to support the organization's continuity of operations plans for key services are identified and established.

Objective TM-2 Protect Technology Assets

Administrative, technical, and physical controls for existing technology assets and those to be acquired or developed are identified, implemented, monitored, and managed.

Practice TM-2.1 ASSIGN RESILIENCY REQUIREMENTS TO TECHNOLOGY ASSETS

Resiliency requirements that have been defined are assigned to technology assets.

Practice TM-2.2 ESTABLISH CONTROLS

Administrative, technical, and physical controls that are required to meet the established resiliency requirements are identified and implemented.

Practice TM-2.3 MONITOR CONTROL EFFECTIVENESS

Controls are monitored for effectiveness and deficiencies are identified and addressed.

Objective TM-3 Manage Technology Asset Risk

Operational risks to technology assets are identified and managed.

Practice TM-3.1 IDENTIFY AND ASSESS TECHNOLOGY ASSET RISK

Risks to technology assets are periodically identified and assessed.

Practice TM-3.2 MITIGATE TECHNOLOGY ASSET RISK

Risk mitigation strategies for technology assets are developed and implemented.

Objective TM-4 Manage Technology Asset Integrity

The integrity of technology assets to support key services is managed.

Practice TM-4.1 MANAGE CONFIGURATION STANDARDS

The configuration items of technology assets are managed.

Practice TM-4.2 PERFORM CHANGE CONTROL

Changes to the IT infrastructure are managed.

Practice TM-4.3 RELEASE MANAGEMENT

The distribution of technology assets to the production environment is managed.

Objective TM-5 Manage Technology Asset Availability

The availability of information assets to support key services is managed.

Practice TM-5.1 CONTROL OPERATIONAL ENVIRONMENT

The environment in which the technology assets are located and operated is controlled.

Practice TM-5.2 MANAGE TECHNOLOGY ASSET MAINTENANCE

Operational maintenance is performed on technology assets as necessary.

Practice TM-5.3 MANAGE TECHNOLOGY CAPACITY

The operating capacity of technology assets is managed commensurate with operational demands to support services.

Practice TM-5.4 MANAGE TECHNOLOGY INTEROPERABILITY

The interoperability of technology assets is managed to avoid service degradation.

Practice TM-5.5 MANAGE TECHNOLOGY SUPPLIERS

Suppliers that provide technology assets or support technology assets for the organization are managed.

Appendix D CERT Resiliency Engineering Framework: Process Management Competencies

The body of knowledge for the CERT Resiliency Engineering Framework Process Management competencies is described on the following pages.

PM – Process Management

PROCESS MANAGEMENT

Purpose

The purpose of Process Management is to establish and maintain a usable set of organizational process assets, improve them based on identified strengths and weaknesses, and quantitatively manage their performance.

Introduction

The scope of this competency area is currently under review. Competency objectives and practices will be developed when this review has been completed.

MA – Measurement and Analysis[22]

PROCESS MANAGEMENT

Purpose

The purpose of Measurement and Analysis is to develop and sustain a measurement capability that is used to support management information needs for managing the resiliency engineering process.

Introduction

The success of security and business continuity activities has been difficult for organizations to express in qualitative terms and nearly impossible to quantify. Traditionally, success has been described as a function of what hasn't happened; in other words, security strategies are seen as effective if the organization has not realized a disruptive event. To some degree, the effectiveness of business continuity strategies is somewhat easier to describe. When an incident occurs that requires the execution of a continuity of operation plan, the organization is able to determine through observation if the plan activities indeed provide an acceptable level of continuity for affected assets and services. However, objective data is rarely collected that would allow the organization to perform detailed analysis on the plan's effectiveness and efficiency. And, for plans that have never been executed in a real-time situation, there is often no success data available.

Measurement and Analysis represents a means for applying metrics, measurement, and analysis to the resiliency equation. This competency represents the organization's application of measurement as a foundational activity in assessing competency and readiness for addressing potential threats and disruptive events and for managing the resulting consequences. The aim of this competency is to apply process improvement techniques to activities like security and business continuity which are typically view from a practitioner level. By elevating operational resiliency to an enterprise process, Measurement and Analysis follows as a necessary capability that forces the organization to decide what needs to be measured, to measure what it can, and use the results to improve the overall posture of the organization.

In Measurement and Analysis the organization establishes the objectives for measurement (i.e., what it intends to accomplish) and determines the measures, quantitative and qualitative, that it believes would be useful to managing the resiliency engineering process as well as to provide meaningful data to management for the processes of governance, compliance, monitoring, and improving processes. The organization collects relevant data (through processes such as Monitoring) and analyzes this data to provide communications to management and stakeholders on trends, progress, success, and areas for improvement.

Related Competencies

EF – Enterprise Focus

MA provides information that management needs to govern and comply with regulations.

MON – Monitoring

MON is a source of data collection that provides data to MA for analysis and reporting.

[22] A significant portion of this competency area is based on the MA process area as described in CMMI models.

Competency Objectives and Practices

Objective MA-1 Align Measurement and Analysis Activities

Measurement objectives and activities are aligned with identified information needs and objectives.

Practice MA-1.1 Establish Measurement Objectives

Measurement objectives are established and maintained based on information needs.

Practice MA-1.2 Specify Measures

The measures necessary to meet measurement objectives are established.

Practice MA-1.3 Specify Data Collection and Storage Procedures

The techniques for collecting and storing measurement data are specified.

Practice MA-1.4 Specify Analysis Procedures

The techniques for analysis and reporting are specified.

Objective MA-2 Provide Measurement Results

Measurement results, which address identified information needs and objectives, are provided.

Practice MA-2.1 Collect Measurement Data

Measurement data is collected consistent with measurement objectives.

Practice MA-2.2 Analyze Measurement Data

Measurement data is analyzed against measurement objectives.

Practice MA-2.3 Store Data and Results

Measurement data, analysis, and results are stored.

Practice MA-2.4 Communicate Results

The results of measurement and analysis activities are communicated to relevant stakeholders.

MON – Monitoring

PROCESS MANAGEMENT

Purpose

The purpose of Monitoring is to collect, log, and distribute important resiliency engineering information to the organization on a timely basis.

Introduction

Monitoring is an enterprise-wide activity that the organization uses to "take the pulse" of its day-to-day operations. It provides the information that the organization needs in order to determine whether it is being subjected to threats and vulnerabilities that require action to prevent organizational impact. Monitoring also provides valuable information about operating conditions that could indicate a need for active organizational involvement.

Many competencies in the Resiliency Engineering Framework implicitly require monitoring capacities in order to achieve higher maturity goals. For example, monitoring provides data about changes in the user environment that can result in necessary changes in access rights and privileges. Or, consider that monitoring contributes to an organization's ability to know when new vulnerabilities emerge (either inside or outside of the organization) or when events or incidents require the organization's attention. This information may require the organization to change its strategy, improve control selection, implementation, and management, or improve the details of its continuity of operations plans. In essence, monitoring is a core competency that the organization must master in order to improve and sustain a level of adequate resiliency.

Monitoring is also a data collection activity that complements process management by allowing the organization to measure process effectiveness across resiliency-related competencies. For example, through monitoring, the organization can determine whether its resiliency goals are being met. It can also tell if its security activities are effective and producing the intended results. In all, monitoring is one way that the organization collects necessary data (and invokes a vital feedback loop) to know how well it is performing in managing the resiliency engineering process.

The Monitoring competency focuses on the activities the organization performs to collect, log, and distribute relevant data to the organization for the purposes of managing threats and incidents and for measuring process effectiveness. To do this, the organization must establish the stakeholders of the monitoring process (i.e., those who have a need for timely information for process management) and determine their requirements and needs. The organization must also determine its monitoring requirements—for managing both operational resiliency and the resiliency engineering process—and ensure that resources have been assigned to meet these requirements. Data collection, logging, and dissemination takes organizational resources; thus the organization must consider and implement an infrastructure that supports and enables its monitoring needs and capabilities. Finally, the organization must collect, organize, log, and communicate the necessary information in a manner that is timely and accurate, and that ensures high data integrity and accessibility.

Related Competencies

EF – Enterprise Focus
MON provides feedback for the purposes of governance and compliance in EF.

VM – Vulnerability Management
MON is a source for information on current vulnerabilities to which the organization is subjected.

IMC – Incident Management and Control
MON provides information about events and incidents that the organization may need to analyze and manage in the incident handling process.

ACM – Access Management and Control
MON provides information related to inappropriate access attempts and or changes in access rights and privileges.

SOM – Security Operations Management
MON is a primary function in the operations activities for security management.

MA – Measurement and Analysis
MON is the function that is a source of data for the purposes of effective process management.

Competency Objectives and Practices

Objective MON-1 Establish the Monitoring Process

The process for identifying, collecting, and reporting important resiliency information is established.

Practice MON-1.1 Identify Stakeholders

The organizational and external entities that rely upon information collected from the monitoring process are identified.

Practice MON-1.2 Establish Monitoring Requirements

The information requirements of stakeholders and resiliency engineering processes are established.

Practice MON-1.3 Assign Resources to Meet the Requirements

Staff are assigned authority and accountability for performing the monitoring activities as necessary to meet requirements.

Objective MON-2 Perform Monitoring

The monitoring process is performed throughout the enterprise.

Practice MON-2.1 Implement and Manage Monitoring Infrastructure

A monitoring infrastructure sufficient for meeting monitoring requirements is implemented and managed.

Practice MON-2.2 Establish Logging Standards and Parameters

The standards and parameters for collecting information and managing information logs are established.

Practice MON-2.3 COLLECT AND LOG INFORMATION

Information relevant to the resiliency engineering process is collected and logged.

Practice MON-2.4 DISTRIBUTE INFORMATION

Collected and logged information is disseminated to appropriate stakeholders.

Appendix E Collaborators

AMD
Richard Reichgut, Senior Manager, Financial Services Strategic Alliance

Ameriprise Financial
Barry Gorelick, Vice President, Ameriprise Business Continuity Management

Bank of America
Andrew McGruden, Senior Vice President, Corporate Business Continuity
Sara Ricci, Vice President, Corporate Business Continuity
Debbie Sanders, Senior Vice President, Corporate Business Continuity
Earlton Singleton, Principal, Global Trading Business Continuity and Operational Risk Lead

Capital Group
Michael Gifford, Resiliency Executive
Bo Trowbridge, Disaster Recovery Coordinator

Citigroup
Gregory Gist, Vice President, Office of Business Continuity

DRII
John Copenhaver, Chief Executive Officer
Michelle Turner, Strategic Alliances Advisor

Discover Financial
Kent Anderson, Technology Risk Management
Rick Webb, Technology Risk Management

Federal Reserve Bank of New York
Todd Waszkelewicz, Supervisory Officer (observation role only)

Financial Services Technology Consortium
Dan Schutzer, Managing Director
John Fricke, Chief of Staff
Charles Wallen, FSTC Managing Executive, Business Continuity Standing Committee

IBM
Eric McNeil, Manager, Corporate Security Strategy
Damian Walch, Resiliency Practice Executive

JPMorganChase
Greg Pinchbeck, Vice President, Treasury and Security Services, Business Resiliency
Judith Zosh, Vice President, Global Technology Infrastructure, Business Resiliency

Key Bank
Shelly Christensen, Corporate Continuity and Recovery
Deborah Minch, Corporate Continuity and Recovery

Charlene Whitcomb, Manager, Corporate Continuity and Recovery

Marshall & Ilsley
Gary Daniels, Vice President, Corporate Business Continuity Planning

Mastercard
Randall Till, Senior Business Leader, Global Business Continuity Management

U.S. Bank
Tom Hirsch, Senior Vice President, Technology and Operations Recovery
Brad Mitchell, IT Manager – Resilience and Recovery
Jeff Pinckard, Technology Recovery Manager
Mike Rattigan, Director, Business Continuity Planning
Mike Stickney, Business Recovery Manager

Wachovia
Brian Clodfelter, Corporate Disaster Recovery Manager, Technology Recovery Services

References

[Ahern 2004]
Ahern, Dennis M.; Clouse, Aaron; & Turner, Richard. *CMMI Distilled: A Practical Introduction to Integrated Process Improvement*, 2nd ed. Boston, MA: Addison-Wesley, 2004 (ISBN 0-321-18613-3).

[Caralli 2004]
Caralli, Richard A. *Managing for Enterprise Security* (CMU/SEI-2004-TN-046). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.
http://www.sei.cmu.edu/publications/documents/04.reports/04tn046.html

[Caralli 2006]
Caralli, Richard A. *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* (CMU/SEI-2006-TN-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.
http://www.sei.cmu.edu/publications/documents/06.reports/06tn009.html

[Chrissis 2003]
Chrissis, Mary Beth; Konrad, Mike; & Shrum, Sandy. *CMMI: Guidelines for Process Integration and Product Improvement*. Boston, MA: Addison-Wesley, 2003 (ISBN 0-321-15496-7).

[Demming 1982]
Demming, W. Edwards. *Out of the Crisis*. Cambridge, MA: MIT Press, 1982.

[Encarta 2006]
MSN Encarta. *engineering*. http://encarta.msn.com/dictionary_/engineering.html (2007).

[FRB 2007]
Federal Reserve Bank of New York. http://www.newyorkfed.org/ (2007).

[Gremba 1997]
Gremba, Jennifer & Myers, Chuck. *The IDEAL℠ Model: A Practical Guide for Improvement*. http://www.sei.cmu.edu/ideal/ideal.bridge.html (1997).

[Kimbrough 1997]
Kimbrough, Tom & Levine, Linda. "The IDEAL Transition Framework – Speeding Managed Change." SEI Symposium, 1997. http://www.sei.cmu.edu/ideal/ideal-presentation.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	May 2007	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Introducing the CERT® Resiliency Engineering Framework: Improving the Security and Sustainability Processes	FA8721-05-C-0003

6. AUTHOR(S)
Richard A. Caralli, James. F. Stevens, Charles M. Wallen, David W. White, William R. Wilson, Lisa R. Young

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2006-TR-009

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-2007-009

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

As security issues dominate news headlines and affect our daily lives, organizations need to improve their ability to protect and sustain their business-critical assets—people, information, technology, and facilities—using human and financial resources efficiently and effectively. Traditional activities such as security and business continuity must not only be effective at achieving these goals but also must offer the organization increased capabilities for managing and controlling operational resiliency. Unfortunately, organizations often manage these activities in a reactive posture fraught with stove-piped organizational structures and poorly defined and measured goals. The result: potentially less-than-adequate operational resiliency to support business objectives. But organizations can vastly improve operational resiliency by viewing it as an engineering-based process that can be defined, managed, measured, and improved. This view ensures collaboration between security and business continuity activities toward common goals and considers the role of supporting activities such as governance, asset and risk management, and financial control. This report introduces the CERT Resiliency Engineering Framework as a foundational model that describes the essential processes for managing operational resiliency, provides a structure from which an organization can begin process improvement of its security and business continuity efforts, and catalyzes the formation of a community from which further definition of this emerging discipline can evolve.

14. SUBJECT TERMS	15. NUMBER OF PAGES
enterprise security management, strategic planning, information security, risk management, operational risk management, process improvement	142

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL