Sustaining Operational Resiliency: A Process Improvement Approach to Security Management

Author
Richard A. Caralli

Principle Contributors
James F. Stevens
Charles M. Wallen, Financial Services Technology Consortium
William R. Wilson

April 2006

Networked Systems Survivability Program

Technical Note
CMU/SEI-2006-TN-009

Unlimited distribution subject to the copyright.

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.

Copyright 2006 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

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).

Contents

List of Figures

List of Tables

About This Report

In December 2004, the Networked Systems Survivability (NSS) program at the Carnegie Mellon® Software Engineering Institute (SEI℠) published a technical note entitled *Managing for Enterprise Security* that described our initial research into process improvement for enterprise security management [Caralli 04a]. In the year since that report was published, we have received numerous inquiries from organizations that are seeking to improve their security programs by taking an enterprise-focused approach. Encouraged by this response, we extended our applied research into enterprise security management and have since expanded our collaboration with industry and government to develop practical and deployable process improvement-focused solutions.

In March 2005, the SEI hosted a meeting with representatives of the Financial Services Technology Consortium (FSTC).[1] Established in 1993, FSTC is a forum for collaboration on business and technical issues that affect financial institutions. At the time of our meeting, FSTC's Business Continuity Standing Committee was actively organizing a project to explore the development of a reference model to measure and manage *operational resiliency* (the ability of an organization to adapt to risk that affects its core operational capacities in the pursuit of goal achievement and mission viability). Similarly, an objective of our work in enterprise security management was to consider how operational resiliency is supported by security activities. Although our approaches to operational resiliency had different foundations (business continuity vs. security), our efforts were clearly focused on solving the same problem: how can an organization predictably and systematically control operational resiliency through activities such as security and business continuity?

To solidify our collaboration, the SEI and FSTC (and its member organizations) joined forces to explore the development of a framework for operational resiliency—with a focus on the core security, business continuity, and IT operations management activities that support it. This technical note describes the results of our collaboration and introduces the concept of process improvement for operational resiliency.

We hope that this work will be another tool in helping organizations to view security and resiliency as processes that they can define, manage, and continuously improve as a way to more effectively predict their ability to accomplish their mission.

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

℠ SEI is a service mark of Carnegie Mellon University.

1 More information on FSTC can be obtained from their Web site at http://www.fstc.org/.

Acknowledgements

The topics of enterprise security and resiliency management encompass a broad range of disciplines and research areas. We have been fortunate to work with many internal and external collaborators who have provided us with the necessary skills and guidance needed to appropriately address these topics.

Many members of the NSS program continue to be invaluable in the evolution of our work. In particular, the authors would like to acknowledge Survivable Enterprise Management (SEM) team members Andy Moore, Carol Woody, and Bradford Willke, who spent many hours analyzing security, business continuity, and IT operations best practices that eventually helped us to frame operational resiliency as a set of essential organization-wide capabilities. In addition to members of the SEM team, we would also like to thank members of the Practices and Development Team, particularly Georgia Killcrece, David Mundie, Robin Ruefle, and Mark Zajicek, who have supported our work and have provided an internal forum for collaboration and discussion.

The authors would also like to acknowledge the special role of William Wilson in advancing this work. As the technical manager for the SEM team, Bill has been our most outspoken supporter, keeping our message alive and viable in light of many challenges we have faced. We realize that new ideas and approaches often come with the responsibility to educate and enlighten. We would not have accomplished as much as we have without his support, guidance, and leadership.

Last, but certainly not least, we would like to thank Rich Pethia for his continuing support of this work. As the NSS Program Director, his desire to “help protect the future of technology” has certainly rubbed off on us and has energized us to make an impact.

We are certainly grateful as well to our collaborators from FSTC and the banking and financial institution community. Your hard work and contributions as well as your seemingly endless knowledge have helped us advance our work immeasurably. (Appendix C provides a detailed list of project participants.) In particular, we would like to thank Charles Wallen, FSTC’s Managing Executive for Business Continuity, for his leadership in bringing these collaborators to our table. In addition, we would also like to acknowledge those individuals who also helped in the development of this technical note: Cole Emerson (KPMG), Barry Gorelick (Ameriprise Financial), Chris Owens (Interisle Consulting), Jeffrey Pinckard (US Bank), Randy Till (Mastercard International), and Judith Zosh (JPMorganChase).

As always, we are grateful to Pamela Curtis for her careful editing of this report and other enterprise security management work and to David Biber, who is always willing and emi-

nently capable of putting our thoughts into meaningful graphics that tell our story better than if we used words alone.

Finally, we would also like to thank our sponsors for their support of this work. We believe it will have impact on our customers' ability to refocus, redeploy, and vastly improve the ways in which they approach security and resiliency in their organizations. It has already had great impact on our customers' ability to improve their security programs and in our ability to transition new technologies in the area of enterprise security management and operational resiliency.

Executive Summary

As organizations face increasingly complex business and operational environments, functions such as security and business continuity continue to evolve. Today, successful security and business continuity programs not only address technical issues but also strive to support the organization's efforts to improve and sustain an adequate level of operational resiliency.

Supporting operational resiliency requires a core capability for managing operational risk—the risks that emanate from day-to-day operations. Operational risk management is paramount to assuring mission success. For some industries like banking and finance, it has become not only a necessary business function but a regulatory requirement. Activities like security, business continuity, and IT operations management are important because their fundamental purpose is to identify, analyze, and mitigate various types of operational risk. In turn, because they support operational risk, they also directly impact operational resiliency.

Because an organization's operating environment is constantly evolving, the effort to manage operational risk is a never-ending task. Critical business processes rely on critical assets to ensure mission success: *people* to perform and monitor the process, *information* to fuel the process, *technology* to support the automation of the process, and *facilities* in which to operate the process. Whenever these productive elements are affected by operational risk, the achievement of the mission is less certain; over time, the failure of more than one business process to achieve its mission can spell trouble for the organization as a whole. Because the risk environment is volatile, an organization needs to maximize the effectiveness and efficiency of its risk management activities. Active collaboration toward common goals is a way to ensure that activities like security, business continuity, and IT operations management work together to ensure operational resiliency.

In practice, organizations have not evolved business models that easily support this collaboration. Funding models, organizational structures, and regulatory demands have conspired to reinforce separation between these activities. One way to overcome this barrier is to view and manage operational resiliency as the end result of an enterprise-owned and sponsored *process*—one that represents the entire continuum of security, business continuity, and IT operations practices working together. With a defined process, the organization can focus on common goals, maximize performance, and ensure that operational resiliency becomes a shared organizational responsibility.

Adopting a process view of operational resiliency provides a necessary level of discipline and structure to operational risk management activities. Moreover, it provides a structure in which best practices can be selected and implemented to achieve process goals. A process view defines a common organizational language and helps the organization to systematically address

compliance and regulatory commitments. Beyond these advantages, a process view of operational resiliency provides opportunities to apply process improvement concepts to security and business continuity activities. A framework for operational resiliency, which describes and defines the processes that are essential for actively and predictably managing operational resiliency, can help organizations to adopt a process view and mature their processes as their operating conditions require. In addition, a framework provides a means for assessing and characterizing the competency of business partners in managing operational resiliency, providing an organization better control over business processes that cross organizational lines.

The importance of managing operational risk will continue to grow as the operational and technical environment of today's organization expands. The emphasis on cost cutting, improving productivity, and gaining a competitive edge requires that organizations use all of their competencies to support organizational drivers and propel them toward their missions. Activities like security, business continuity, and IT operations management must be active contributors to this effort. But current approaches to managing these activities as separate and disconnected approaches to support will continue to be a drag on organizations' limited resources and will not produce the intended effect: to support and sustain operational resiliency.

The convergence of these activities is not just a foundation of our theories and assertions but is a natural outgrowth of the risk management connection between these activities. But convergence requires collaboration, and organizations will need to overcome deeply ingrained cultural and funding barriers to guarantee it. We see the introduction of a process approach—led by security management—as a promising way for organizations to operationalize these theories and inculcate a process improvement mindset. A process improvement approach enables organizations to actively direct and control operational resiliency rather than be controlled by it.

Abstract

Organizations face an ever-changing risk environment. The risk that emanates from the day-to-day activities of the organization, operational risk, is the subject of increasing attention, particularly in the banking and finance industry, because of the potential to significantly disrupt an organization's pursuit of its mission. Security, business continuity, and IT operations management are activities that traditionally support operational risk management. But collectively, they also converge to improve the operational resiliency of the organization—the ability to adapt to a changing operational risk environment as necessary. Coordinating these efforts to sustain operational resiliency requires a process-oriented approach that can be defined, measured, and actively managed. This report describes the fundamental elements and benefits of a process approach to security and operational resiliency and provides a notional view of a framework for process improvement.

1 Introduction

Two years ago, on the heels of several years of fieldwork in using and training the CERT® OCTAVE® method, we began to more closely examine the field of security and the ways in which security activities are defined and carried out in organizations. Through analysis of security practices and security approaches, our focus became clear—at its core and in all of its forms, security should be treated and managed as just another type of operational risk management activity, with the goal of supporting the organization's operational resiliency. Over the same period, other communities were drawing similar conclusions about activities like business continuity and IT operations management and service delivery.

This technical note describes our continuing research into helping organizations control and improve operational resiliency by refocusing their security, business continuity, and IT operations management activities via a process-improvement approach.

1.1 Background

The results of our previous research in the area of enterprise security[2] management (ESM) were published in a preceding technical note entitled *Managing for Enterprise Security* [Caralli 04a]. This research area evolved from our fieldwork in developing and transitioning information security risk assessment methodologies. As we worked with customers to improve their risk assessment and mitigation capabilities, we observed that they could make temporal, locally-optimized progress at the operational unit level but lacked success in having long-term, organization-level impact. Much of this was attributed to the insufficiency of organizational-level security processes and risk management activities. In other words, we found little (if any) support for security as an enterprise-wide process, with the result that organizations are unable to sustain and build on localized successes. A common example of this is the lack of a process for developing, implementing, maintaining, and enforcing an enterprise-wide security policy. Often, operating unit-level risk mitigation strategies and controls (such as discouraging password sharing) were observed as ineffective because of the lack of policy management at the enterprise level.

Another outgrowth of this fieldwork is the observation of a disturbing trend: the tendency of organizations to define security success as the absence of a disruption or event. Those re-

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

® 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 methodology can be found at http://www.cert.org/octave.

[2] The use of the word "security" is intended to be broadly inclusive of such activities as information security, network security, physical security, and in the case of people, safety.

sponsible for the security of the organization—whether focused on information, technology, facilities, or even people—tend to describe their achievement in terms of what hasn't happened instead of expressing success in terms of goal achievement and capability.

In our first technical note, we expanded on and translated these observations into a description of the evolution of security as a series of shifts toward a broader, enterprise view.[3] In that note, security is described as an activity moving away from technically focused and reactive activities to a *process* that is adaptive, enabling, and enterprise-focused. In effect, to mature the security discipline, it must connect with organizational drivers and be institutionalized as an organizational process that can be actively controlled, measured, and improved. We stopped short of suggesting a specific solution or methodology to facilitate this emerging view; however, we identified a set of notional capabilities that represent the fundamental activities that contribute to the security process and its success.

Since our first technical note was published, we have refined our research to focus on the security-operational resiliency connection—to give security the organizational direction and importance it needs—and to the application of process improvement concepts to security. Through examination of widely accepted best practices in the areas of security, business continuity/disaster recovery, and IT operations management,[4] we have refined and expanded our list of notional capabilities so that they represent the collaboration of these activities toward a common goal. And we have begun the development of a framework to capture a process improvement approach to security and operational resiliency.

1.2 Moving Toward Operational Resiliency

As organizations face increasingly complex business and operational environments, functions such as security continue to evolve. Today, a successful security program is one that not only addresses technical issues but strives to support the organization's efforts to improve and sustain a level of adequate *operational resiliency*. Operational resiliency is the ability of the organization to adapt to risk that affects its core operational capacities—business processes, systems and technology, and people—in the pursuit of goal achievement and mission viability. Supporting operational resiliency is the emerging target for security, business continuity, and IT operations management because together they help the organization to manage operational risk—a type of risk that can significantly impede or even stop an organization's quest to accomplish its mission.

---

[3] Refer to Section 2 of *Managing for Enterprise Security* for a detailed description of these shifts.

[4] "IT operations" defines the scope of activities that are performed to develop, deliver, and manage IT services for the organization. The Information Technology Infrastructure Library (ITIL) is an increasingly popular set of best practices that defines a process view of controlling and managing IT operations. It covers IT service delivery, service support, and security management. When we speak of IT operations management, our point of reference is ITIL.

1.3 Operational Risk Management as the Driver

Managing operational risk is paramount to mission success. For the banking and financial services industries in particular, operational risk management is essential because of operational complexity, the interdependencies between financial institutions and their business partners, and the foundation that these institutions provide for the United States banking system and economy. For these reasons, the Basel Committee on Banking Supervision [Risk-glossary 06a] continues to bring the subject of operational risk management to the forefront in the boardrooms and executive offices of many major corporations. Whereas organizations were once resigned to accept operational risk as a necessary evil of doing business, it is now an essential focus of the organization and in some cases, a regulatory requirement.

Because operational risk management is a fundamental aim of security, business continuity, and IT operations functions, those functions are receiving higher visibility in organizations than ever before. Technical innovations and a shifting sociopolitical landscape have introduced new complexities that outpace the development and implementation of approaches to address an expanded risk environment. Unfortunately, heightened awareness has not translated into higher levels of effectiveness. While organizations acknowledge the importance of risk-based activities, they continue to manage them without shared goals or processes—the goals of the activity are prioritized over the needs of the enterprise. This affects the organization in many ways, including

- inadequate goal setting for security, business continuity, and IT operations activities
- duplicated effort across functions and departments
- inadequate or incomplete identification of risk
- less than optimal mitigation of risk (to benefit the entire organization)
- increased overall risk management costs

1.4 An Evolving Process View

Organizations deploy many sets of best practices to facilitate their security, business continuity, and IT operations management activities. These best practices have a useful purpose: they provide the organization an experience-based set of activities, often with a proven track record of success, that can help them manage on a daily basis. But a best practices approach does not necessarily equate to goal achievement or success. In fact, organizations that use common best practices may have set no goals at all. They also may not be aware when a best practice is ineffective or when a best practice is actually costing them more to operate than the benefits they achieve by deploying it. Unfortunately, using best practices alone to manage a discipline such as security often defaults to a “set and forget” mentality—the organization turns its attention away from the practices once they have been implemented.

But consider the difference with a process view. A process view serves as a baseline description of expected practice and results at the organizational level. It requires active management and goal setting. It defines a high-level path to a set of enterprise goals, often traversing

many different departments and operational units. The process can be measured, and when out of control, actions can be identified and implemented to bring it back in control. A process view provides a structure in which best practices can be more effectively selected and utilized to ensure goal achievement. And unlike a best-practices-only approach, a process view can define and enable collaboration between activities that are traditionally divided along organizational, functional, or categorical lines—as is needed for managing operational resiliency.

1.5 Scope of this Report

This technical note intends to accomplish several things:

1. Build on earlier work in enterprise security management and the evolution toward process improvement.
2. Define operational resiliency as the target for security and other operational risk management-based activities.
3. Describe the essential link between security, business continuity, and IT operations management.
4. Describe the fundamental elements and benefits of a process approach to security and operational resiliency.
5. Provide an advanced view of a framework for process improvement.
6. Describe the rationale for a benchmark for operational resiliency in the banking and finance community.
7. Establish an open dialog with the community for input and shaping of an eventual process improvement model.

It is important to note that, while operational risk management is a key area of focus, this technical note is not intended to suggest a process for managing operational risk. Operational risk management is a broad and sometimes poorly defined activity that may not lend itself to process definition. Instead, we intend to focus on the interrelationships between security and other activities that each must address some aspect of operational risk, with the intent to improve the overall focus on operational resiliency.

1.6 Structure of the Report

This document has three distinct purposes: to provide background on our ongoing research, to present our initial findings and observations, and to describe a notional model for process improvement for operational resiliency. The sections of this document are arranged around these purposes as follows:

- Introduction and background – Sections 1 and 2
- Fundamental elements – Sections 2 and 3

- Notional process improvement framework description – Sections 4 and 5
- Collaboration and future research – Sections 6 and 7

Additional related information such as taxonomy and relevant practice sources is included in Appendices A and B.

1.7 Target Audience

The intended audience for this technical note is people and organizations who have an interest in improving their security programs and operational resiliency. Knowledge of risk management and familiarity with the emerging subject of resiliency is helpful to digest our arguments regarding the connection between security and other operational risk management activities. Those who have knowledge of process improvement, particularly in the software engineering discipline, will begin to see emerging analogs in the delivery of security services across an enterprise.

Before reading this technical note further, it is helpful, but not necessary, to familiarize yourself with our previous work in this area. This can be found in the technical note *Managing for Enterprise Security* [Caralli 04a] and in other various papers and presentations in the "ESM" section on the CERT green portal at http://www.cert.org/nav/index_green.html. These artifacts provide a collective history of our emerging thought regarding security process improvement.

2 Operational Resiliency Defined

With good reason, organizations are actively examining how well they can handle adversity and still accomplish their goals. Disruptive events are waiting around every corner—technology can fail, people can make mistakes, adversaries can attack, and disasters, both natural and manmade, can strike quickly. Simply being aware of these potential disruptions is not enough; the organization must be able to operate under adverse conditions and have the capacity to return to normal as quickly and cheaply as possible. In short, the organization must make itself sufficiently *resilient* to disruptions if it intends to remain viable.

2.1 What is Resiliency?

While it might seem to be the buzzword of the moment, the term *resiliency* is not new. In the scientific community, resiliency has long been understood to be a property of a physical material such as steel and rubber.[5] Specifically, it defines the ability (or inability as the case may be) of these materials to return to their original shape after they have been deformed in some way. Physical materials have degrees of resiliency. For example, flat-rolled steel, used to form the bodies of cars, isn't particularly resilient—once it has been dented or creased, significant effort is required to return it to its original shape, if that can be done at all. Rubber, on the other hand, is inherently resilient—a tennis ball takes quite a beating during a match, but at rest, it usually returns to its familiar spherical shape.

As the term resiliency has permeated other disciplines and industries and has been applied to other objects such as people, its meaning continues to evolve. A good example is in the educational psychology field, where resiliency refers to the ability of people to bounce back from adversity. Regardless of how the term is applied or in what industry or discipline it is used, we have identified three basic elements that traverse most definitions. To describe the property of resiliency for any object, you must describe its ability to

1. change (adapt, expand, conform, contort) when a force is enacted
2. perform adequately or minimally while the force is in effect
3. return to a predefined expected normal state whenever the force relents or is rendered ineffective

Thus, the degree to which an object is resilient is dependent on how well it performs across the entire life cycle of a disruption—from point of impact, while under duress, and after the disruption goes away.

[5] See WordNet definition at http://wordnet.princeton.edu/perl/webwn?s=resiliency.

2.2 Organizational Resiliency

Given the risk environment in which most organizations operate today, it is easy to see how the term *organizational resiliency*[6] has evolved. Organizational resiliency describes the competency and the capacity of the organization to adapt to dynamic and diverse risk environments. A resilient organization is capable of changing and adapting before its environment forces it to do so [Hamel 03].

Organizational resiliency is dependent on how well the organization manages a broad array of disruptive events[7] and risks that emanate from all levels and functions in the organization. These risks could result from

- changes to overall business climate and environment (such as short supplies of raw materials or a rise in the cost of a basic commodity such as energy)
- changes in the social, geographical, or political environments in which the enterprise operates
- disruptions to upstream and downstream value chains (such as vendor instability and changes in customer base)
- emerging threats to technical and network infrastructures (that may be caused by hacking, denial of service attacks, or espionage and spying)
- insider threat and fraud (related to disgruntled employees or collusion with external parties)
- events over which the organization has little control, such as natural disasters

Theoretically, organizational resiliency represents the organization's cumulative competency for managing resiliency across all organizational activities and functions—the places where risks emerge. Organizational resiliency *results* when the organization's critical strategic and operational business functions or processes—ranging from strategic planning to supply chain management to IT operations and security management to financial management—are resilient. A lack of resiliency in any of these critical business functions or processes directly affects overall organizational resiliency.

2.2.1 Characteristics of organizational resiliency

Simply describing organizational resiliency as the ability to adapt to changing risk environments is not entirely useful. Besides realizing that resiliency is a property rather than an activity, from a practical standpoint, there are several characteristics of resiliency that an organization must consider.

---

[6] For our purposes, organizational resiliency is functionally equivalent to the term *enterprise resiliency*.

[7] We define a disruptive event as any event that has the potential to affect the ability of the organization to meet its core mission.

1. **Resiliency requires a comprehensive view of risk.** A resilient organization is competent at managing the identification of potential threats as well as in preparing to deal with the impact of these threats if they are realized. In other words, resiliency is dependent on managing both the conditions and consequences of risk across the entire organization.[8] For example, an organization can improve its resiliency by developing a plan to operate critical business processes if a critical technology component (such as a server) is lost. However, a higher degree of resiliency is achieved if the organization combines its continuity plan with active identification and prevention of threats (through implementation of administrative, physical, and technical controls) that could affect critical technology components. A comprehensive view boosts the organization's resiliency by addressing risk from both perspectives.

2. **Resiliency requires an expanded view of the organization.** Few organizations can operate without extending their operational environment to include external partnerships. Indeed, the popularity of outsourcing continues to support, if not promote, this reality. However, there is a downside: while these partnerships are necessary to achieve goals, they can also provide a great source of additional risk. Success in achieving the mission of organizational business processes is often predicated the resiliency of a chain of partners that extends outside of the organization's physical boundaries. Thus, an organization that is truly resilient must recognize that resiliency must be achieved not only in every layer of the organization, but also as the organization extends to its external business partners and customers. To ensure an end-to-end resilient value chain, the organization's risk management expertise must be extensible to this expanded view.

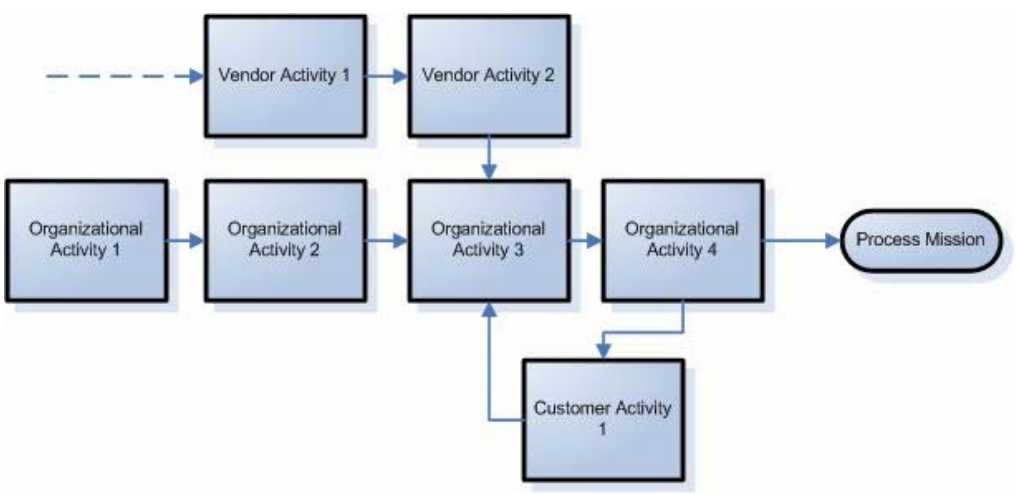

Figure 1: An expanded target for resiliency

3. **Resiliency requires more than meeting operational goals.** Organizations can consistently meet their operational goals and be drawn into a false sense of resiliency as a result. Many organizations perform admirably for years, meeting analysts' expectations and returning shareholder value. Then a disruptive event such as a hurricane or flood

[8] This includes all types of risk, including strategic risk, legal risk, market risk, and operational risk.

hits, and the organization is no more. And what about the organization that sets inadequate goals that are easily reached? Goal achievement in this case says nothing about the organization's resiliency. Goal achievement alone, even if the goals are well defined, will not help the organization's viability if it has not considered the potential effects of a disruptive event and prepared—both proactively and reactively—to address it.

4. **Measuring resiliency is difficult.** Metrics such as profitability and customer response time can be unambiguously measured, and these measurements can be used as indicators of the organization's overall health. But for resiliency often all that can be measured is how well an organization performed in the past when an event has occurred. Thus, measuring an emergent property such as resiliency requires active monitoring and measuring of many different indicators that would predict success in avoiding disruptive events or coping with them when they do arise.

5. **Resiliency is dynamic.** The resiliency of an organization is constantly changing and adapting as the complex environment around the organization changes. For some organizations, this is as rapid as minute to minute. Thus, resiliency is not something that an organization achieves and then forgets; the organization must apply continual effort to remain agile and prepared. This requires not only that the organization strive for operational excellence but that it is consistently good at identifying and mitigating risk. It is a never-ending pursuit, and the target—operational resiliency—is a moving one.

2.3 Operational Resiliency

To some degree, organizational or enterprise resiliency is conceptual—it is difficult to actively manage because it results from doing all of the right things at every level of the organization. But active contributions to organizational resiliency can be made by managing resiliency at all functional levels of the organization. For example, consider a car production line: cross training all personnel to perform more than one function on the production line means that the organization is more resilient to fluctuations in resources. When resiliency is considered at the *operational* level, organizational resiliency can be actively influenced, supported, and enabled.

2.3.1 Operational resiliency defined

Operational resiliency describes the organization's ability to adapt to and manage risks that emanate from day-to-day operations. Organizations that have resilient operations are able to systematically and transparently cope with disruptive events so that the overall ability of the organization to meet its mission is not affected. From a practical standpoint, operational resiliency means designing and managing business processes and all of their related critical assets—people, information, technology, and facilities—in a way that ensures the process mission is achievable and sustainable as risk environments change. Thus, operational resiliency results from active management of the resiliency of critical organizational assets.

2.3.2 Foundations of operational resiliency

Functional operational resiliency is a balancing act that the organization must become very adept at managing. At this point of equilibrium, there is a convergence of many organizational demands that must be actively considered. On one hand, the organization is balancing the resources and assets that it deploys to reach its goals against its desire to keep costs contained and maximize return on investment. At the same time, it must consider the level of resources it is willing to expend to ensure that disruptive events—the kind that could pull it off course in reaching its goals—are prevented or limited in the type and extent of damage that they can do to the organization. On an aggregate scale, many organizations do not do this systematically; instead, they generally find out that they have failed to balance these competing demands properly when it is too late.

To approach operational resiliency from a strategic standpoint, organizations must attempt to answer two questions:

1. What is the normal operating state of the organization?
2. What level of operational resiliency is adequate for the organization?

The operational equilibrium

Disruption of any type impedes the organization's ability to reach its goals. The extent to which a disruption becomes a critical issue for the organization depends on how much tolerance the organization has for operating away from the norm.[9] For example, a virus that is introduced to an organization's email system potentially disrupts productivity. If the disruption is minor, the organization will probably not notice; on the contrary, if it is major, the organization may be unable to perform routine operations. Being able to define *normal* provides a benchmark against which the organization can decide how resilient it is against a range of impacts.

Organizations have a theoretical operating comfort zone where there is equilibrium between the resources they deploy and their production of products or delivery of services at the most efficient cost. At this point, the missions of critical business processes are being achieved and are contributing to the organization's mission. Products are being produced and services are being delivered at the least possible resource utilization. And reasonable value, in the form of profits or other benefits, is being returned to stakeholders. Disruptive events that manifest from risks exert forces that potentially move the organization away from this theoretical equilibrium. Whenever this occurs, there are generally negative effects on the organization, such as

- Additional costs are incurred.
- Production or service goals are impeded.

[9] To some degree, this is the same as defining the organization's risk tolerance. Higher risk tolerance may mean that the organization is more comfortable (or more capable) of operating further away from the norm and for a longer period of time. A lower risk tolerance may limit how far and for how long an organization can operate away from normal.

- Return on investment is less than expected given operating conditions.
- Other organizational effects are realized (reputation is damaged, fines and legal penalties are levied, health and safety of employees and customers is affected, etc.).

An organization must decide, based on many factors including its organizational drivers and risk tolerances, how much movement away from equilibrium it can accept. Slight, daily variations from normal may be tolerable, but extreme movements can stifle the organization and even cause it to cease operations. Today, there are many examples of entire industries that are very sensitive to market forces and environmental risks. Consider the airline industry—some airlines can absorb increased fuel costs for an extended period of time, but for others, this is the operating expense that will finally cause them to go out of business. Another example is Internet-based businesses—an extended denial-of-service attack shuts down their ability to connect with customers. Dealing with this condition for just a few days could strike a fatal blow.

The point of operational equilibrium is important because it is the baseline for describing the range of tolerance that an organization has to disruptive events. In turn, this range essentially describes the limits of an organization's operational resiliency. Consider a tightly-wound spring. When the spring is stretched, there is a point at which the spring will break. This breaking point is as far away from normal as the spring can operate. An organization that can operate within a large range of deviation from normal might be more operationally resilient than an organization that has tighter limits (this is illustrated in Figure 2).

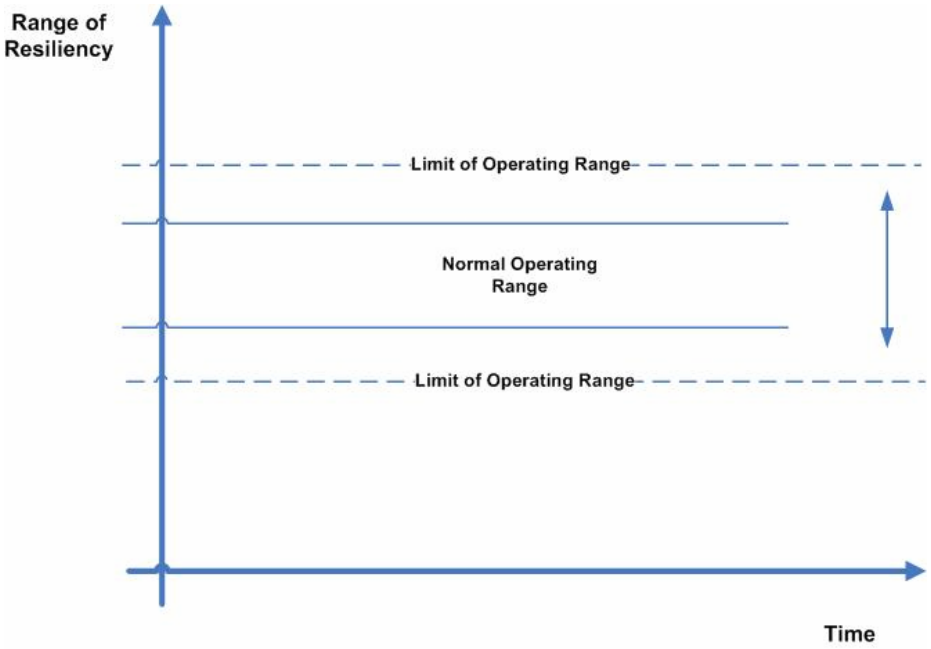

Figure 2: Simple illustration of range of operational resiliency

Adequate operational resiliency

Can an organization be too resilient? The answer is "yes" if the organization expends efforts to become more resilient than is necessary based on the range of fluctuation it can accept from normal operations.

Adequate operational resiliency describes the point at which the organization is expending just enough resources to ensure that it can maintain its range of tolerance from normal and still accomplish its mission. Like a fingerprint, an adequate level of operational resiliency is unique to each organization because it is based on many diverse factors such as mission, industry, geographical location, competitive position, level of technology usage, and regulations and laws. It can also be dependent on other factors. For example, if an organization's core business is to provide services to another business—much like a backup data center might provide services to a bank—it may need to have a higher level of operational resiliency to meet its obligations. Or, if an organization has a significant cash reserve, it might be able to tolerate longer periods of low earnings or higher temporary costs due to disruptive events or risks.

The level of adequate operational resiliency is also dynamic. Just as the risk environment for an organization constantly changes, so does the meaning of "adequate." What is adequate for meeting an organization's mission today may change drastically tomorrow. Socioeconomic conditions, changes in political climate, fluctuations in the prices of raw materials such as oil, and even consumer trends can immediately wreak havoc on an organization's ability to adapt to risk. In addition, as organizations introduce more complexity to operations, particularly in the area of technology, the risk environment becomes more dynamic, often due to integration issues that form new pathways for risk to develop. Thus, adequate operational resiliency requires the organization not only to be competent in dealing with deviations from normal but also to realize that *normal* is redefined sometimes on a daily basis.

Figure 3 is a notional illustration of the concept of adequate operational resiliency.

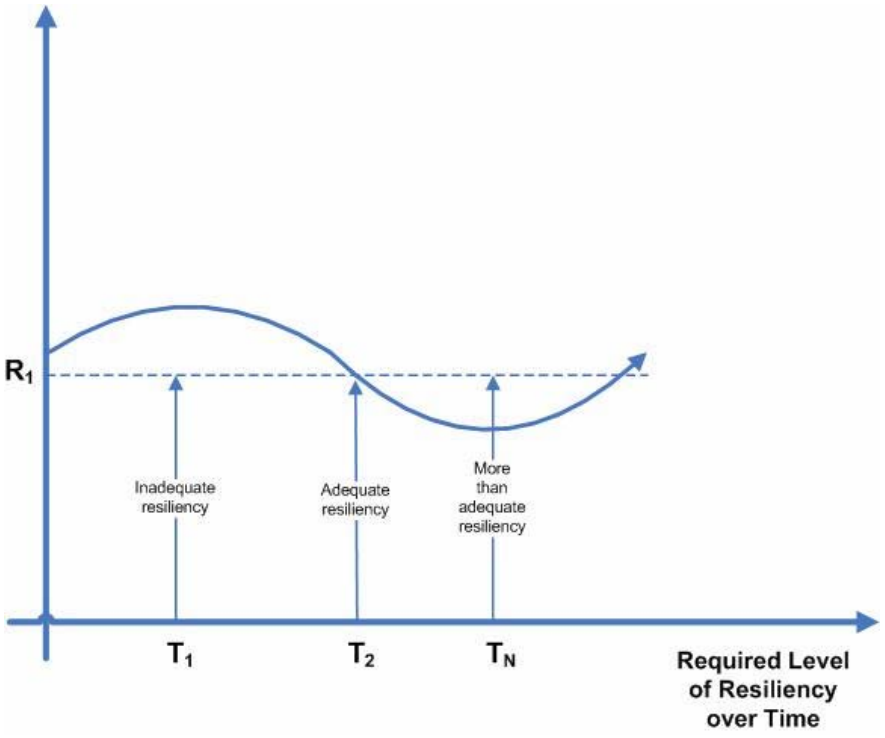

Figure 3: Simple illustration of adequate operational resiliency

In summary, an operationally resilient organization must have the capacity and capability to achieve three things:

1. To the extent possible, implement controls and processes to prevent or limit forces from moving the organization away from normal.
2. Be able to survive during an extended or significant movement away from normal until the disruption relents or is eliminated.
3. Most importantly, have the capacity and capability to enable a return to the normal state.

In other words, the organization must be able to efficiently and effectively expend the resources necessary to prevent disruption, operate[10] during disruption, and restore operations to normal. The inability to perform any one or all of these tasks diminishes the organization's operational resiliency.

2.4 Operational Resiliency and Risk

The subject of risk is never too far from a discussion of operational resiliency. In fact, operational resiliency depends on how well the organization adapts to risk—in particular, operational risk.

[10] *Operate* in this context means ensuring that critical business processes continue to achieve their mission, albeit in a diminished form. The organization must remain mission-focused during any deviation from normal operating conditions.

2.4.1 Operational risk[11]

Simply stated, *operational risk* is the potential for loss that arises from the day-to-day operations of an organization. According to the Basel Committee,[12] operational risk can be defined as the risk of loss resulting from [Riskglossary 06b]

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

Operations defines a very large part of what an organization does: it is the recurring activities that directly or indirectly support the organization's core mission. Operations can range from product assembly and accounting to marketing and human resources management. Because of the broad definition of operations, the source and extent of potential risks can be overwhelming, if not unmanageable. In an attempt to bound operational risk, the Basel Committee offers seven standard categories of events that could result in operational risk and result in losses to the organization. They are

1. internal fraud
2. external fraud
3. employment practices and workplace safety
4. clients, products, and business practices
5. damage to physical assets
6. business disruption and systems failures
7. execution, delivery, and process management

With such a broad potential for organizational disruption, controlling operational risk is the new burden of management. Once considered to be an unpleasant side effect of doing business, failure to acknowledge operational risk in today's complex operating environment can be fatal. This is best highlighted by the banking and finance industry—focusing on credit and market risks is important to meeting strategic goals, but a failure to control operational risk could contribute to a systemic failure of the United States banking system and, by association, the United States economy.

[11] This technical note is not intended to be a primer on operational risk. However, it is important to understand aspects of operational risk in order to understand its connection to operational resiliency.

[12] In January 1999, the Basel Committee proposed a new capital accord known as Basel II. It redefines the basic capital requirement for banks as an expression of not only credit and market risk, but operational risk as well. The effective date for implementation of Basel II is December 2006, so organizations must quickly improve their capabilities for identifying and mitigating operational risk.

2.4.2 Operational risk and resiliency

It would be misleading to say that organizations have until now ignored operational risk; on the contrary, while they may not have a specific operational risk management function, it is likely that they have addressed aspects of operational risk through security, business continuity, and IT operations activities that they perform on a routine basis. And by doing so, they also likely have considered, albeit accidentally, that operational resiliency depends on how well they use these activities to holistically manage operational risk. In other words, the extent to which they manage and balance the risk equation[13]—condition and consequence—is an influential factor in how well they manage operational resiliency and in how resilient they are.

In Section 3, we consider how the convergence of these three activities—security management, business continuity, and IT operations management—are key drivers for attaining and sustaining an adequate level of operational resiliency.

2.5 Resiliency Versus Survivability

Finally, the prevalent use of the term survivability, particularly in the area of security, requires an attempt to differentiate it from resiliency as described in this technical note. Survivability is the ability of a system to fulfill its mission in a timely manner in the presence of attacks, failure, or accidents [Ellison 97]. Although traditionally focused on systems, when extended to the organization survivability describes the collaboration between the protection of information assets and systems and the management of business risks [Fisher 00].

Resiliency can be viewed as an extension of the concept of survivability. Resiliency describes the essence of survivability—the need to accomplish the mission in the face of adversity—but extends this definition to explicitly include risk prevention as well as restoration of normal processes once a disruption has relented.[14] Beyond survivability, resiliency is an expanded concept describing the flexibility of objects to adapt to their changing environment—to *thrive* in such an environment, not just to survive an attack. From a systems perspective, resiliency considers the interdependencies between systems and the complexities of a system of systems. In the context of an organization, true resiliency means effective management of this adaptation with minimal effect on mission and at the least overall cost to the organization. In essence, from an organizational viewpoint, resiliency is the institutionalization of the concept of survivability.

---

[13] Risk management is certainly a complex field, and there are many definitions of risk. In general, risk entails exposure and uncertainty. From a security perspective, it is often useful to think of risk in terms of threat, vulnerability, impact, and probability. The potential that a threat actor will act on a vulnerability, resulting in an undesirable outcome, essentially defines a risk. We can simplify this definition for our purposes (with help from the field of software risk management) by describing risk as a **condition and a consequence**. In other words, a **condition**—vulnerability potentially acted upon by a threat agent—and a resulting **consequence** (if the condition occurs) poses a risk that the organization must address.

[14] In some cases, depending on the material, resiliency may also describe the property of a material to get *stronger* as a result of having had forces exerted upon it.

3 Operational Resiliency as the Goal

Operational resiliency is an ongoing challenge for an organization. Clearly, it is impacted by nearly every activity that the organization performs (or fails to perform). Some effects on operational resiliency are indirect: ensuring employee health and well-being is good business sense, but also supports operational resiliency. Other activities have a more direct impact on operational resiliency. Security management, business continuity planning, and IT operations management *directly* support an organization's operational resiliency because their fundamental purpose is to identify, analyze, or mitigate various types of operational risk. A convergence of these activities can significantly influence, if not improve, the organization's operational resiliency goals.

To explore this assertion, it is important to understand how each of these activities helps the organization to attain and sustain an adequate level of operational resiliency.

3.1 Security Management

Security is a vastly misunderstood organizational competency. It comes in many forms—information security, physical security, and network security, to name a few—that share a common goal: to provide critical assets with a desirable degree of *safety*,[15] or freedom from danger, injury, or risk. Depending on your definition, security activities can range from implementing access control lists for systems to installing padlocks on file room doors to developing and implementing policies. *But the common thread that permeates all security activities in an organization is the focus on managing risk.*

Security activities are in reality often just an extension of risk management activities: the identification, analysis, and mitigation of risk that could affect the organization's critical assets. Security activities do this by focusing on the entire risk equation—both conditions (which manifest in vulnerabilities and threats) and consequences (which impact the organization). This broad focus is what gives security activities meaning and importance to the organization. Table 1 provides a basic summary of the security activities performed to address both the condition and consequences of risk.

[15] Just like resiliency, safety is a property of an object (such as a critical asset) that results from managing risk. It could be said that an organization that is sufficiently operationally resilient has provided an acceptable degree of safety for its critical assets.

Table 1: Relationship between security activities and risk

Risk Element	Security Activity
Condition	Identification of possible vulnerabilities and threats to critical assets through risk identification and analysis activities
Condition	Limitation of exposure by development and implementation of technical, administrative, and physical controls
Consequence	Development and implementation of plans to prevent, reduce, or limit impact of realized risk to an acceptable level

Effective security management requires a holistic view of the entire risk equation to ensure protection of critical organizational assets by limiting exposure of critical assets to risk, reducing the unwanted effects on the organization when risk is realized, or both. When an organization does this effectively—in alignment with organizational drivers and at the lowest possible cost—it is directly supporting operational resiliency.[16] In essence, operational resiliency is the reward for effective risk management brought about by effective security management.

But security activities alone cannot sustain operational resiliency. Today's business model is technology and collaboration heavy, and thus security shares responsibility for risk management with business continuity and IT operations management.

3.2 Business Continuity

Like security, business continuity is difficult to define and describe. Depending on the organization, business continuity activities can range from developing and implementing contingency plans for critical application systems and business processes to responding to and managing operations during a disaster or crisis. *However, the basis for business continuity is the organization's desire to limit the unwanted effects of realized risk.*

The recent resurgence of business continuity as an essential part of organizational planning is predicated on the increase and near-catastrophic results of well-publicized events such as terrorist attacks and natural events such as hurricanes. But the importance of business continuity is also an outgrowth of the recognition of this activity as a core risk management contributor and as such, it has by necessity evolved and matured into an enterprise-wide competency.

There is significant overlap between business continuity and security management because both address aspects of operational risk. While security management tends to focus more heavily on the conditions for risk, business continuity has traditionally been a consequence-driven activity.[17] But organizations that have matured their business continuity efforts under-

[16] It is also likely to be satisfying the security objectives of critical information assets—confidentiality, integrity, and availability.

[17] Some organizations would argue with this characterization. For them, business continuity is catalyzed by business impact analysis, which serves to identify potential risks as a way to determine what type and extent of continuity planning needs to be performed. However, acknowledgement of

stand that the lines between security and business continuity are less well-defined than ever (as they should be). Business continuity requires a consideration of risk so that impact-reducing activities can be planned for the assets that are most important to meeting the organization's mission. For example, where should the organization concentrate its planning? Should the training department receive the same focus as payroll? Security is concerned with the same questions. The risks that form the basis for solid and organizationally-driven business continuity plans also provide the basis for selecting and implementing risk prevention and mitigation controls, traditionally the focus of security. Good business continuity management is an extension of the security discipline because risk is the catalyst for both. The failure of many security and business continuity programs often traces back to separation of these functions to the extent that they are operating on different assumptions. When they converge, however, holistic management of operational risk is possible and the resulting effect is an improvement in operational resiliency.

3.3 IT Operations Management

Technology is an undeniable part of how organizations operate today. It supports the productivity of the organization's critical business processes and assets. But it also introduces increased complexity that often results in new and undiscovered pathways of risk. In fact, it is one of the richest sources of operational risk—so prominent that most organizations define their security and business continuity programs around technology-driven activities.

The complexity and pervasiveness of technology is fueling the growth of IT operations management as an emerging and vital organizational process. The increasing popularity of frameworks such as the Information Technology Infrastructure Library (ITIL) supports not only the importance of the process but recognizes the contribution it makes to the organization's overall viability.

The requirements for IT operations management come from two primary sources: the organization's need to sustain the availability of technology to support business processes and the security requirements of information and technology assets. To satisfy these requirements requires a broad array of skills and functions such as managing a help desk, managing changes and configurations, identifying and analyzing incidents, and monitoring effectiveness. But a secondary and equally important goal of IT operations management is to manage and control operational risks—those that are inherent in the use of technologies such as the Internet. For example, installing software patches on a regular basis keeps software up to date and reduces exposure to known vulnerabilities that have been already identified and addressed.

It is no accident that organizations that improve their IT operations capabilities often reap residual improvements in security and continuity. This is because effective IT operations

---

the importance of thoroughly examining the condition of risk as a driver for business continuity is often found only in organizations that have realized the benefits of coordinating security and business continuity efforts.

management supports higher levels of technology availability. The prominent role of technology in carrying out business processes means that higher availability translates into direct improvements in operational resiliency as well.

3.4 A Convergence of Operational Risk Management Activities

In practice, mission success for the organization relies on mission success of each business process. Mission success for a business process is dependent on sustaining the productive capacity of critical objects that the process needs: people, information, technology, and facilities. Whenever the productivity of any of these objects[18] is impaired, the mission of the business process can fail. Failure of more than one business process simultaneously can spell irreversible trouble for the organization.

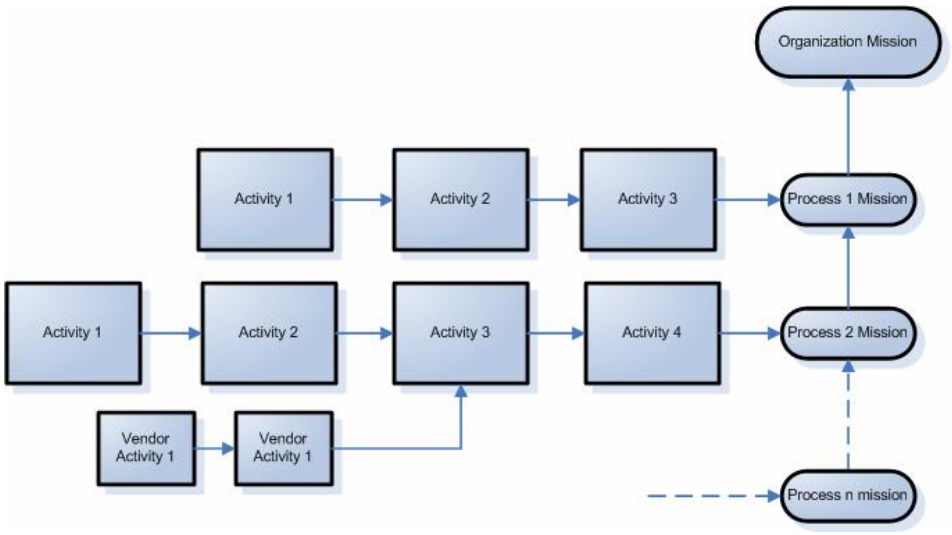

Figure 4: Process mission supports organizational mission

By themselves, security management, business continuity, and IT operations management are essential organizational activities because they sustain the productivity of critical business process objects. But when coordinated—by focusing on the same risks and aiming at the same goals—they become a powerful enabler of operational resiliency as well.

3.4.1 A coordinated view

In summary, the dependencies between security, business continuity, and IT operations activities are clear, even if organizations don't explicitly manage them collaboratively. Notwithstanding their support for operational resiliency, there are plenty of reasons to consider these activities collectively.

[18] More detail on these objects and their importance to a process improvement framework is provided in Section 5.

- **They share common practices.** Scan the bodies of best practices in each discipline and you will see significant overlap between them. Security practices make mention of business continuity. IT operations practices include security references. These overlaps are not accidental; in reality, the lines of demarcation between these practice sets are vague at best. Rather than existing as three separate disciplines, the best practices of security management, business continuity, and IT operations can be seen as a continuum of practices that are aimed at effective operational risk management and support for operational resiliency. By design, organizations have separated these functions to facilitate management, but doing so is actually counterproductive to reaching their individual goals.
- **They focus on the same objects—people, information, technology, facilities, and business processes.** The desire to keep these objects productive is why security, business continuity, and IT operations practices are worthy of funding by the organization. Each activity focuses on either limiting exposure to risk, managing the effects of realized risk, or both.
- **They are driven by the same requirements.** The requirements for these activities come from the same source: the organization's drivers and critical success factors. This establishes what critical objects and business processes are important to the organization and provides the foundation for which risks need to be addressed. Operational resiliency is diminished when activities like security and business continuity are predicated on different assumptions about what critical objects are important.
- **They share common goals and outcomes.** Common requirements result in common, shared goals. Regardless of whether they are performed individually or collaboratively, security, business continuity, and IT operations have the same organization-level goals, including sustaining operational resiliency.

Thus, operational resiliency can be seen as a product of collaborative security, business continuity, and IT operations management (see Figure 5). With operational risk as the foundation, collaboration provides a synergistic effect that strengthens each individual discipline and optimizes results for the enterprise at the lowest possible cost and best utilization of resources. It ensures that these activities are performed with a shared and consistent strategic and organizational view. And, most importantly, it ensures that these activities converge on a common goal: to help the organization attain and sustain an adequate level of operational resiliency.

Figure 5: Foundation for operational resiliency

3.4.2 From theory to reality

Envisioning operational resiliency as the end product of this collaboration is easier than implementing it as such. Organizations recognize that enterprise goals (such as operational resiliency) require dedicated coordination and communication to achieve, but they are usually not functionally structured to enable such an effort.

In our opinion, one way to overcome this barrier is to change how operational resiliency is viewed. Operational resiliency is the end result of an enterprise-owned and sponsored *process*—one that represents the entire continuum of security, business continuity, and IT operations activities working together. With a defined process, the organization can ensure a focus on common goals and maximize resource deployment in achieving these goals. In short, a process view eliminates the dependency on operational unit performance; instead, operational resiliency becomes the responsibility of everyone in the organization.

4 A Process Approach to Operational Resiliency and Security

The demands on an organization's limited resources—human and capital—are greater than ever before. In addition to continuously improving profitability and returning value to stakeholders, organizations must deal with regulators, be good corporate and community citizens, and fund research and development, all in an environment of uncertainty. Every task in an organization is under constant examination for how well it returns value for its investment. It is no wonder that activities like security and business continuity—generally considered necessary evils—are often good candidates for extracting costs.

But what if security management, business continuity, and IT operations management could be activities that actually enhance an organization's bottom line? What if the investment in these activities could bring a measurable return to stakeholders? The answers to these questions are important because improving the value proposition for these activities depends strongly on elevating the importance of their contribution to the organization.

Security and other risk management activities do not necessarily have to be inefficient or high cost. However, to improve their efficiency depends on being able to actively manage them. Because organizations do not view activities like security management as processes, they do not deploy the tools and knowledge that could enable cost elimination and improved goal achievement. Now that it is no longer elective for organizations to improve security and operational resiliency, they must find ways to be more effective with the limited resources they have to spend. They must make security and business continuity part of the culture. They must optimize IT operations to drive down operational risks in technology and improve security. They must do so before regulators tell them to or prescribe *how* they must do it. In our opinion, they must move to a process view of operational resiliency.

4.1 Describing a Process Approach

A process is a structured collection of related activities aimed at reaching a desired outcome. There are many organizational processes; some are defined and known by the organization, and others are informal, poorly defined, and unable to be communicated. When an organization has a defined process, it is more likely to bring about the desired results because a roadmap for accomplishing goals is developed and communicated. Consider for example a basic organizational process: submitting and paying an expense report. Employees would have difficulty submitting expenses for payment if there weren't a process for them to follow. In the absence of a defined process, employees would create their own way of submitting expenses, causing increased effort and costs for the organization, as well as diminished effectiveness.

The lack of a controlled process might also result in increased fraud or reduced accuracy. What organization can afford these effects?

In much the same way, failure to recognize security and related activities as processes can create similar chaos and expense—people in the organization don't see themselves as integral to the process, there is no defined way of reaching goals, there is no way to know when the goals have not been reached, and worse yet, the organization cannot diagnose what has gone wrong and how to fix it. Unfortunately, this is the state of security and business continuity in many organizations today, and it contributes to the inability to answer questions like "Is the organization secure?" and "Is the organization resilient?" Too often, the answer can only be given in the absence of data: "Nothing has happened; therefore we must be doing it right."

4.1.1 Definition of a process approach for operational resiliency[19]

A process approach to operational resiliency is described as the means for defining, communicating, and controlling the process used by the organization to support and sustain a level of adequate operational resiliency. It establishes shared operational risk management goals. It aligns and relates the necessary activities to support security, business continuity, and IT operations goal achievement and alignment. It provides a means for the organization to predictably and systematically collaborate to accomplish these goals. By taking a process view, the operational risk management thread that is pervasive across these activities is solidified.

Our progress to date in defining elements of a process approach to operational resiliency is included in Section 5.

4.1.2 Benefits of a process approach

Unfortunately, organizations today are swimming in a sea of frameworks, best practices, regulations, and other advice that purports to help them reach their security goals. Yet organizations continue to struggle for success. A process view of operational resiliency brings many advantages that incorporate common practice and helps organizations develop roadmaps for success. They include

- focusing on common goals and requirements

[19] Why is our focus on operational resiliency and not specifically security? Our aim in this technical note is to frame security as an important driver of operational resiliency. Certainly, our work to date has shown that security must be viewed in the context of operational resiliency to be valuable to the organization. Thus, it is our current belief that a process improvement approach to security is the same as a process improvement approach to operational resiliency. In other words, the critical element for improving security is to manage it in the larger context of operational resiliency. The same could be said of business continuity. Only with IT operations do we suggest otherwise. IT operations and service management is a broad field with requirements that emanate from many aspects of the organization. We include IT operations as a driver for operational resiliency because it is foundational for both security and business continuity. Thus, we include aspects of it in our process view. However, we recognize that a process improvement approach to IT operations management would be much broader than what we are defining in this technical note.

- eliminating organizational barriers to goal achievement
- defining and communicating security and business continuity processes
- measuring effectiveness
- providing structure for best practices
- defining a common language
- easing compliance and regulatory commitments

The following sections describe each of these benefits in more detail.

Focusing on common goals and requirements

An organization must ensure that the factors driving its success are known and communicated so that risk can be considered in the context of those factors. Security and business continuity[20] activities must be built on these factors to ensure the resiliency of the most important organizational assets. A process view of operational resiliency establishes and enforces this common focus toward the intended outcome of sustaining operational resiliency.

Figure 6 provides a notional view of how operational resiliency requirements are derived from organizational drivers and form the basis for risk-based activities in the organization.

Eliminating organizational barriers to goal achievement

As mentioned previously, organizations tend to compartmentalize functions like security and business continuity (and certainly IT operations management, which is naturally the domain of the technology organization.) While this may have evolved from an ease-of-management perspective, once ingrained in an organization it creates political and turf barriers that are not easily overcome. Collaboration in an organization is an expensive activity, so it is often easier, less costly, and less problematic to manage these functions in separate operational units. But risk management is a process that traverses the enterprise, depends on many organizational capabilities, and is more effective when focused on enterprise needs. A process approach to operational resiliency aims to break down these organizational barriers by having the organization focus on the process and intended outcome (as a primary objective) rather than where the activities are performed and by whom. The process becomes the focus, and the integration between risk-based activities is built in to ensure sharing of resources, goals, and performance. When the process is the focus, the organization can adjust its execution and performance in any way that best fits the organization's cost structure and culture, so long as the intended outcome is achieved. And viewing security and business continuity as enterprise processes elevates them to the level of importance that is required for success.

[20] Because IT operations activities are vitally connected to security management and business continuity, by default they also derive requirements from organizational drivers, particularly in the sense of which technology assets are important and the availability requirements for those assets.

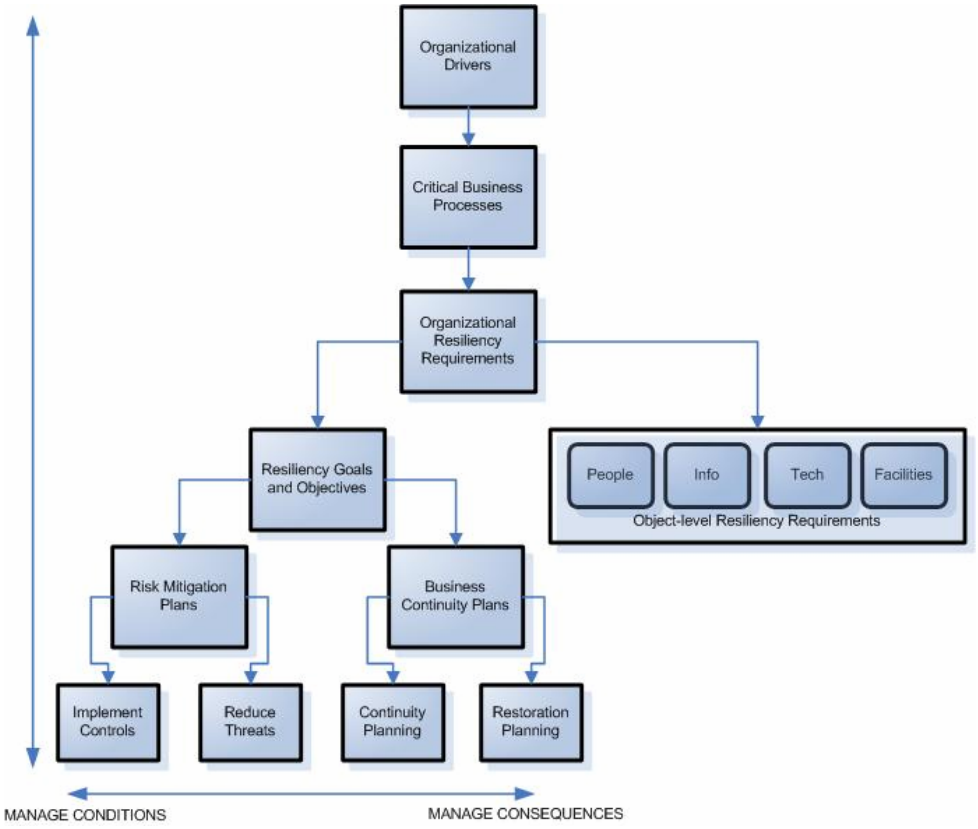

Figure 6: Requirements cascading from organizational drivers

Defining and communicating security and business continuity processes

In many organizations, it is difficult to define exactly what security entails, particularly when it crosses into the business continuity space or when IT operations activities are satisfying security requirements. When an enterprise-wide process is accurately described or defined, the organization is able to

- know where the process begins and ends
- describe what is to be accomplished
- assign resources such as people and equipment commensurate with needs
- communicate the process to those who have direct or indirect responsibilities and those who may need to know, particularly those outside of the organization that may be involved
- identify the direct and indirect costs of achieving the goals of the process
- ensure that everyone is working within the process and toward the same outcomes
- facilitate collaboration across organizational barriers

Thus, a process definition for operational resiliency provides the linkages between the vital security, business continuity, and IT operations activities that must share responsibility for success.

Measuring effectiveness

One of the biggest problems facing organizations today is the ability to demonstrate the value of operational risk management activities. As the importance of these activities grows, organizations tend to continue to fund them based on current events or anecdotal evidence of effectiveness rather than defining meaningful metrics and collecting measurements. It certainly is tempting to call a security program a success if there is no evidence of hacking or to feel good about business continuity plans if they have been successful in the past. But what if the event is something that the organization has yet to encounter?

Organizations have become complacent in accepting the measurement of effectiveness of risk management activities in the absence of data. Therein lies the advantages of a process view—a process that can be defined can also be controlled and measured. 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. 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 investment has value or whether the end result of the process is achieved—they can measure it.

Providing structure for best practices

Best practices help and hurt organizations at the same time. On the one hand, best practices 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 their peers. On the other hand, best practices tend to be prescriptive, and once organizations "take their medicine" they tend to believe that there is nothing else they need to do.

Another potential problem of best practices is that there are so many of them. Not only do industry groups create them, but many are generated by regulatory bodies to enforce specific behaviors through compliance. Best practices also tend to be activity specific, which often solidifies the organization's inclination for drawing organizational lines between them. Organizations that approach operational risk management through a best practice approach soon find that they have many different sets of practices to manage and integrate—and that they have chosen practices that may not necessarily bring about the intended result.

A process perspective turns the organization's focus to the *outcome* of the process (see Figure 7). 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. 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 set of practices. Instead, the organization can turn its attention to ensuring that the practices used are effective for supporting process goals.

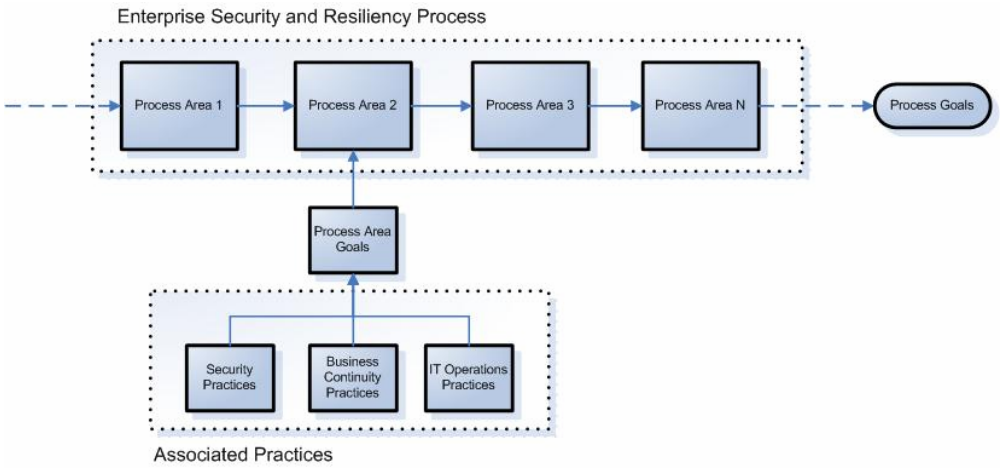

Figure 7: Process versus practice

Defining a common language

The definition of *taxonomy* is "a division into ordered groups or categories."[21] Without a structured taxonomy, it is difficult for a culture—whether it is a particular industry, a community of researchers, or a group of friends—to communicate. Imagine how difficult it would be to describe the vast landscape of plants and animals if everyone used a different naming convention and definition.

A common taxonomy for security and business continuity (or other risk-based activities) has been elusive to date. As emerging disciplines, their language continues to evolve from a technology perspective. However, the elevation of these activities to an enterprise level and the need to collaborate requires a common way of communicating. An advantage of a process view of operational resiliency is that, because it requires a process definition, it can also be a catalyst for the definition and communication of a common language.

Easing compliance and regulatory requirements

Organizations spend considerable resources interpreting regulations and devising a strategy for compliance. Unfortunately, this often requires that they divert their attention from achieving their goals and objectives in order to satisfy regulatory bodies. A process approach may help to ease compliance burdens by giving organizations a systematic and more efficient way to determine compliance gaps. In addition, because regulatory requirements are a fundamental input to the resiliency process, compliance may naturally follow as an output of managing the process. By virtue of having a defined process to review, regulators wanting to get a more definitive read on an organization's competency in a particular discipline may also be satisfied more quickly, rendering them less likely to implement additional regulatory guidelines.

[21] *The American Heritage® Dictionary of the English Language*, Fourth Edition

4.2 Considerations for Process Maturity

One of the benefits of model-based process improvement is the ability to benchmark an organization's current level of capability. Based on their unique requirements and objectives, organizations can determine if they need improvement and can develop plans to close the gap between current performance and expected performance. For a process aimed at operational resiliency, this concept could help organizations take a disciplined, systematic approach to improving their security and business continuity efforts and in improving the collaboration with other risk-based activities. The ability to rate an organization's process maturity has certainly been an advantage of model-based process improvement as is exhibited in the Software Engineering Institute's Capability Maturity Model® framework for software engineering. But as in the software discipline, there is also some potential for abuse. An organization using such a model may seek a particular maturity rating in order to qualify as a preferred contractor rather than to realize the benefits of process maturity and improvement. Translated to the security or business continuity disciplines, this could have disastrous results. Instead of speaking to an organization's capability for managing security, a maturity level could be misread as implying how secure an organization is at a point in time. For example, one might incorrectly conclude that an organization that achieves a higher level of process maturity is more secure than an organization that achieves a lower level. In reality, the difference in these levels speaks only to an organization's competency in consistently reaching its security goals, not how secure it is currently. And lower levels of competency may in fact be acceptable for an organization given its unique operating context. Thus, an organization that exhibits more maturity in security or business continuity is not necessarily secure or resilient; instead, it is more *capable* of achieving its security and resiliency requirements.

As process improvement techniques are introduced into security and resiliency, the proper use of process maturity concepts will require more attention and deliberation so that they can become a meaningful element of an organization's process improvement efforts.

4.3 Notional Process Maturity for Operational Resiliency

It would be presumptuous on our part to try to describe a model for evolutionary maturity of an organization's operational resiliency process capability at this time. Even though we have identified notional capabilities that describe this process, we have not yet performed enough research to know how and if these capabilities should be staged to describe process maturity. However, we have performed enough basic research and fieldwork to describe notionally how the conversion to a process view potentially improves an organization's overall maturity with respect to operational resiliency.

In our previous technical note, we described four notional approaches that organizations use for the security management process. Without assigning capabilities or processes to each of

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

these notional "levels," we attempted to describe their characteristics. In essence, our aim was to provide an early scale that organizations could use to describe their current approach and to determine if this approach is adequate given their organizational drivers. Our original levels were calibrated and named based on the primary characteristic—ad hoc, vulnerability based, risk based, and enterprise based. However, as we began to expand these descriptions to account for the collaboration of security management with other risk-based activities and the focus on operational resiliency, we found that these naming conventions were not as purposeful. We translated our notional descriptions into a more process-oriented view, choosing to downplay the activities performed at the notional levels and focusing instead on the degree to which a process is defined, measured, and managed. Thus, we updated our notional description of four levels of approaches to managing operational resiliency as a process—lack of process, partial process, formal process, and cultural.[22] Our future work related to process maturity for operational resiliency will use these descriptions as a foundation. Each is described in more detail below.

4.3.1 Lack of process

A lack of process is characterized by a recognizable absence of a systematic means for defining and achieving operational resiliency requirements. Security is approached by dealing with disruptive events as they occur, often characterized by individual heroics. There is no active consideration of business continuity planning. The organization is simply coping and has no tangible plan for action. There are ambiguous lines of responsibility and authority for security management and funding is sporadic and event driven. Security and resiliency goals and requirements are not actively determined, and when they are, are not based on organizational drivers. There is no oversight of security or business continuity activities and no course correction when goals are not being set or achieved. People are the most important resource, if not the only resource involved.

4.3.2 Partial process

An organization that recognizes the importance of a disciplined means for achieving operational resiliency requirements may be characterized as having a "partial process" approach. But operationally it still carries out security and business continuity activities along functional lines rather than taking an enterprise view. There is a focus on identifying vulnerabilities in the technical infrastructure because the organization views security and business continuity as IT's responsibility. There is some implicit awareness of organizational drivers but the process is still focused on events. Funding for these activities is still sporadic and considered to be an expense or burden to the organization. There is informal governance over the poorly defined process.

[22] Thanks to help from http://www.betterproductdesign.net/maturity.htm for providing a working set of generic categories.

4.3.3 Formal process

A formal process is characterized by explicit organizational recognition of a systematic means for achieving defined operational resiliency goals. The organization is able to repeat success (i.e., fend off threats and fully recover business processes with limited organizational impact) because there is active learning. The process spans the enterprise and is implicitly aligned with organizational drivers so that the focus is on the critical assets and objects that are most important to the organization. Not everyone in the organization is aware of or acculturated to the process, but responsibility and accountability for core activities is well defined, even if it is misplaced (i.e., in the IT department only). Security management and business continuity activities are still considered to be expense driven. There is informal governance of the process, but there may be a chief risk manager or similar role overseeing the process for the enterprise.

4.3.4 Cultural

A cultural process is fully inculcated in the organization's culture. Everyone in the organization is aware of the process and their roles and accountability for the success of the process in meeting goals. The process is defined, performed, and managed, and the organization is easily able to know and repeat its successes. The process is measured to ensure it is meeting its goals and improved where gaps are identified. The process spans the enterprise and is not "stuck" in the domain of one or more functional areas—there is a true enterprise-wide collaboration. The focus of the process is on the objects of security and resiliency—people, business processes, technology, information, and facilities—so that the entire range of disruptions is considered. The process is owned by the organization and the goals of the process are explicitly aligned to organizational drivers through a formal process. The organization uses many capabilities and processes spread throughout the organization to accomplish its goals. There is formal governance and feedback is directed toward process improvement.

4.3.5 Increasing levels of competency

While our notional description of process evolution does not necessarily describe process maturity, it has helped us to identify some evidence of improvement (albeit anecdotal at this point) in operational resiliency as an organization moves toward more defined processes. From our experience, organizations that move away from event-driven approaches to security management and resiliency toward more formal and cultural processes exhibit a better ability to bring an enterprise focus to a discipline such as security that is traditionally relegated to operational units. It also begins to give the organization more active and predicable control over meeting security goals (see Figure 8).

From a security perspective, we have concluded that the move toward viewing and managing security as a process potentially cures many of the current ills that affect complex organizations in their desire to make security a value-driven activity and in improving its effectiveness. Thus, as the organization moves toward a defined security process, it moves away from viewing security as a technical activity focused on survivability to one that has an enterprise

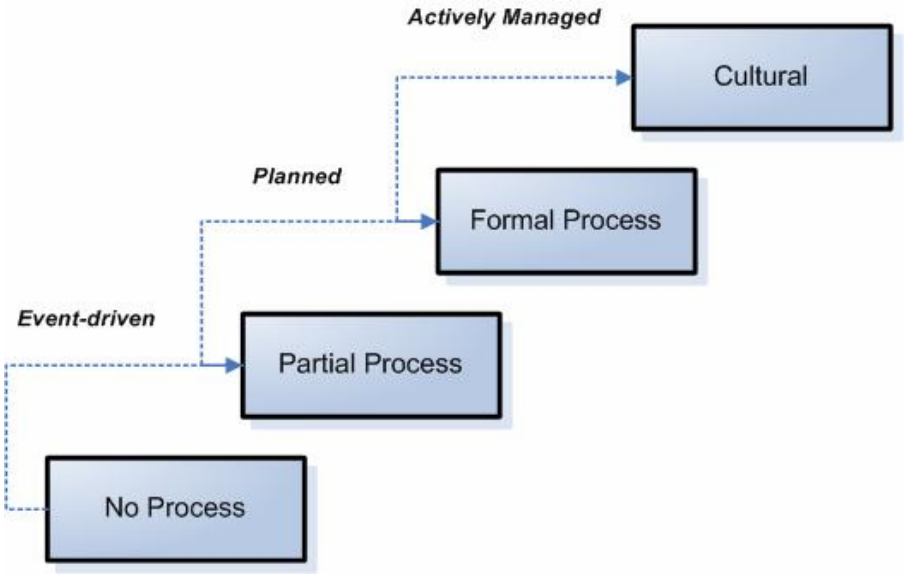

Figure 8: Increasing levels of competency through a process view

focus that sustains and improves operational resiliency. Security and resiliency in this view become systematic and adaptive processes that are contributors to the organization's strategic posture (see Figure 9).

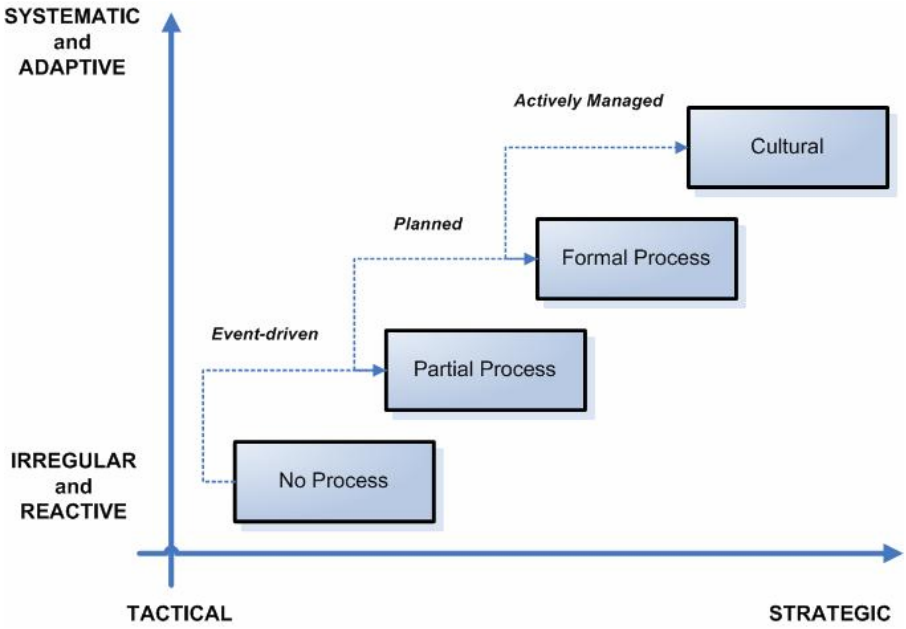

Figure 9: Moving toward continuous improvement

5 A Process Improvement Framework for Operational Resiliency and Security

Much of our research in the past two years has focused on identifying and analyzing the challenges facing organizations that want to improve (make more efficient and effective) their security efforts. From this initial exploration of the problem space, we have turned our focus on developing tools, techniques, and methods for security and operational resiliency process improvement. An initial work—the critical success factors method—was developed in 2004.[23] The critical success factors method is our first attempt to give organizations a way to explicitly identify, document, and express their organizational drivers in terms of success factors—both internal and external to the organization—that must be consistently achieved in order to accomplish their mission. An organization can use these success factors as a foundation to ensure that efforts such as security and business continuity are focused on what is important to the organization.

Our most current work involves the initial development of a process improvement framework that represents and defines a process approach to managing security and business continuity with a focus on operational resiliency. In essence, the framework strives to bring these activities together to provide a predictable and controllable approach to sustaining operational resiliency. Developing such a framework is an intricate process, so we have been very careful in taking smaller steps and validating our assumptions along the way. This section describes the work we have done to date as a foundation for progress toward a fully functional process improvement model in the future.

5.1 Establishing the Framework

To develop our initial description of a framework, we have concentrated our efforts in collecting relevant data through these activities:

- fieldwork
- practice mapping and analysis
- application of commonly understood process improvement concepts

[23] The critical success factors method is documented in an SEI technical report called *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* [Caralli 04b].

5.1.1 Fieldwork

We have been fortunate over the years to work with organizations in the private and government sectors to analyze security effectiveness and to apply security tools and techniques. Our recent experiences with methodologies like OCTAVE have provided a wealth of information about the challenges and barriers to effectiveness in managing security toward accomplishment of a set of organizationally driven goals. Through fieldwork, we have been able to capture what organizations do effectively in managing security; conversely, and perhaps more importantly, we have also been able to observe what organizations are not doing well. Through critical examination of these observations, we have been able to shape our assertions regarding a process approach to operational resiliency and to capture information on essential processes and capabilities.

5.1.2 Practice mapping and analysis

Fieldwork and research continue to form the foundation of our process approach to security and resiliency, but clearly we also recognize the value of an established community of practices to guide our work, particularly in the identification of essential capabilities and processes. As mentioned earlier, there is certainly no lack of standards, practices, and guidelines available for information security and related disciplines—this is clearly evident in the 81 sets of best practices documented by the Corporate Information Security Working Group [CISWG 04]. As our focus has expanded to operational resiliency, we continue to add new sources of practices to our target list, particularly in the areas of business continuity and disaster recovery. Our current list of relevant best practices is provided in Table 2 and is described in more detail in Appendix B.

Since our previous technical note was published in January 2004, we have completed an initial mapping of various best practices into affinity groups that have helped us to identify essential processes and capabilities. In addition, through this exercise we have

- confirmed our assumptions on the shared focus on operational risk and resiliency
- identified the common focus on five objects or assets (see Section 5.3.1)
- identified our initial set of capabilities that define a process for security management (see Section 5.3.2)

The following table describes each of the practice sets with which we have become familiar and have used in our affinity analysis activities. The expansion of our work into the business continuity realm through our collaboration with the Financial Services Technology Consortium (FSTC) has also added to our list. We will continue to add relevant practice sets as necessary to ensure a robust consideration of all essential organizational capabilities and processes.

Table 2: Sources of practices

Source	Audience	Focus	Relevance to ESM
BS7799/ISO17799	International	Information security management	Management of information security practices
CobIT	International	IT security and control	Control objectives for information technology security and process control
ITIL	International	IT service management	IT service and operations management practices that contribute to security
ISF-The Standard	International	Information security	Information security practices
NIST 800-14/800-53/FIPS 200	Mostly U.S.	Information systems security	Information security practices that are focused on systems
HIPAA	U.S.	Data security	Information security practices that are focused on information and data
CMMI & other maturity models	International	Process improvement	Structure for process improvement and maturity
DRII Professional Practices	International	Business continuity and recovery	Business continuity and disaster recovery practices sponsored by certification body Disaster Recovery Institute International
DRJ Generally Accepted Business Continuity Practices	International	Business continuity and recovery	Generally accepted business continuity practices

5.1.3 Application of process improvement concepts

We continue to seek collaboration with a community of process improvement practitioners through interaction with Carnegie Mellon® Software Engineering Institute (SEI) personnel involved in the development and support of the Capability Maturity Model Integration (CMMI) Product Suite and CMMI users. Familiarity with the CMMI framework and its various instantiations has provided candidate process areas and capabilities that need to be considered for inclusion in or integration with the process improvement framework for operational resiliency. In addition, because of the importance of people to operational resiliency, other models such as the People CMM contain relevant process areas that are topical for consideration in our framework.

5.2 Creating a Framework

All of our experiences as detailed above are aimed at the development of an initial process improvement framework for operational resiliency. In the past several months, we have developed a design outline that captures data collected from each of these experiences. We are currently engaged in translating this data into a high-level framework that can serve as the catalyst for exploring and developing an eventual process improvement model.

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

In Section 5.3, the initial candidates for inclusion in a process improvement framework are presented. These capabilities are likely to be subject to significant recasting and reformulation after the publication of this technical note, so this information is presented for descriptive purposes only at this time.

5.3 Elements of a Notional Framework

The following sections describe two important elements of an eventual operational resiliency framework: objects on which the framework is focused and the initial identification of capabilities.

5.3.1 Framework objects[24]

As noted previously, there are five essential objects that an organization depends on to accomplish its mission: people, information, technology, facilities, and business processes (Figure 10). These objects are also often the target of operational risk management—a disruption in the productive deployment of any of these objects has the potential to interfere with or significantly impact the organization's ability to carry out its day-to-day operations and accomplish its mission. Consider an information asset such as the design specifications for a critical product line: if a disgruntled employee destroys these specifications, there is a potential that the production process will be delayed or, at worst, the product can never be produced again. Depending on how prepared the organization is for such an event, this disruption could be a minor irritation, an expensive loss of production, or the event that puts the organization out of business.

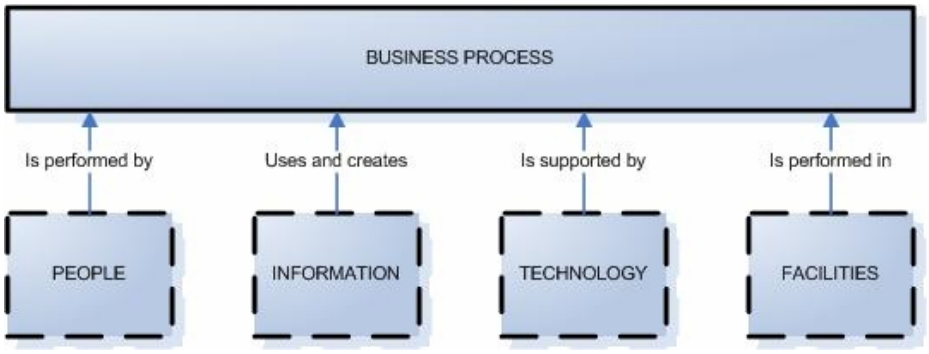

Figure 10: Five objects of operational resiliency

An organization performs security activities primarily for the purpose of preventing disruption to the productive capability of these objects. Business continuity activities are performed to ensure that the business processes that rely on objects such as people, technology, information, and facilities can continue to operate in the event that they are disrupted. In total, these activities sustain operational resiliency by sustaining the resiliency of each object.

[24] The word *asset* can be substituted for object.

People

People are the human capital of the organization. There are few business processes that operate without human intervention, either in an active manner or in a monitoring capacity. People use the other framework objects—information, technology, facilities, and business processes—to achieve goals. People are an important component in sustaining operational resiliency, but are often the most complex asset to manage.

Information and data

Information is a critical organizational asset. It is a raw material that is used by business processes to achieve their individual missions. It is also often produced by business processes.

Technology

Technology assets directly support the automation (and efficiency) of business processes. For some organizations, technology is a prominent factor 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.

Facilities and physical plant

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. Physical protection of facilities often provides an important layer of protection needed to ensure the operational resiliency of the other objects.

Business processes

Business processes are the foundational engine that keeps the organization running. Business processes can range from support processes such as accounting and legal to those processes that are directly involved in the production of products or the delivery of services. Business processes contribute to the organization's ability to accomplish its mission; critical business processes must each achieve their individual mission in order to contribute to the overall mission.

An important aspect of the business process object is that all of the other objects are directly related to it. 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 use in the process and to be produced by the process
- *technology* to automate and support the process
- *facilities* in which to perform the process

5.3.2 Capability areas and proposed capabilities

Capability areas are broad categories that describe the basic building blocks for a process improvement approach to managing the security, business continuity, and operational resiliency of organizational objects and assets. They define the high-level scope of the process and provide meaningful categories in which to describe the process capabilities. To date, we have identified eight working capability areas:

1. Enterprise
2. People
3. Technology Assets and Infrastructure
4. Information and Data
5. Physical Plant
6. Resiliency Relationships
7. Service Delivery
8. Resiliency Sustainment

In each of these capability areas, we have also defined notional capabilities. For the purposes of our framework, a capability is described as a competency that contributes to the organization's ability to approach security and operational resiliency as a process and to achieve security and operational resiliency goals in a systematic, disciplined, and predictable manner. Proposed capabilities defined to date are included under each of the capability areas described below.[25]

Enterprise

The Enterprise capability area includes processes that address the sponsorship, support, and promotion of an enterprise view of security and resiliency. These capabilities ensure that operational resiliency is a strategy-driven process and that there is an explicit connection between security goals and the resiliency requirements of the organization based on its strategic drivers—mission, purpose, values, vision, goals, objectives, and critical success factors.

The Enterprise capability area is an explicit acknowledgement of the need for the organization to sponsor security and resiliency and to provide direction for these efforts through the identification and satisfaction of operational resiliency requirements. In this view, resiliency

[25] The list of capabilities itemized and described under each capability area is not intended to be all-inclusive or complete. They represent our work to date and will form the basis for translation to a process improvement framework. Additional capabilities are under consideration and may be incorporated in future work. Another important point of clarification: although there is often similar language used, the capabilities we have defined are not intended to represent key process areas as would be seen in CMMI or other CMM models. At this point, capabilities are used to collect and define the functions that represent essential security, business continuity, IT operations, process management, and organizational management activities. As we begin to develop our first iteration of a framework, these capabilities will be subjected to much review and revision.

goals are derived from organizational and operational goals, thereby setting the correct context for security, business continuity, and IT operations activities and managing the potential impact of risk. This requires an explicit focus on the underlying business processes of the organization that are critical to achieving the organization's mission.

Table 3 describes proposed capabilities for the Enterprise capability area.

Table 3: Enterprise capabilities

Capability	Short Description
Enterprise Focus	Focus security and resiliency at the enterprise level and ensure it is founded on the organization's drivers.
Strategic View	Ensure explicit alignment between security and resiliency planning and delivery and the strategic planning, goals, and objectives of the enterprise.
Resiliency Governance	Establish an enterprise-level oversight process for the security and resiliency programs and service delivery.
Resiliency Standards and Policies	Establish and enforce acceptable security and resiliency behaviors.
Resiliency Planning	Establish a planning process for security and resiliency that aligns with strategic planning assumptions and goals.
Resiliency Requirements Management	Set security and resiliency goals and deliver service to satisfy enterprise security and resiliency goals.
Risk Foundation	Establish risk management and mitigation as the foundation for security and operational resiliency and as a driver for resiliency decisions and actions.
Compliance Management	Establish an enterprise-wide coordinated approach to identifying and complying with relevant legal and regulatory requirements through operational security and resiliency activities.
Business Process Management	Inventory and prioritize enterprise mission-critical business processes and establish them as the focus of enterprise security and resiliency planning and service delivery.
Resource Management	Allocate and manage sufficient monetary resources to achieve enterprise security and resiliency goals.

People

The People capability area represents processes that focus on the human resources of the organization and how they contribute to achieving security goals and sustaining operational resiliency. The scope of this capability area includes not only the general employee population but also security, business continuity, and IT operations personnel whose primary focus and area of responsibility in the organization is directly related to sustaining resiliency. In addition, crucial issues of employee viability, particularly during an event or crisis (such as family and emotional and physical well-being) are considered.

Table 4 describes proposed capabilities for the People capability area.

Table 4: People capabilities

Capability	Short Description
Workforce[26] Competencies	Identify competencies and skills necessary to deliver security and resiliency services and to achieve security and resiliency goals, and determine gaps.
Workforce Management	Manage resiliency workforce to sustain necessary competencies and skills and to ensure an adequate level of performance commensurate with meeting resiliency requirements.
Workforce Training	Establish process to provide ongoing training to workforce to increase competencies for delivering resiliency services and achieving resiliency goals.
Personnel Management	Establish and maintain the contributions necessary from the general workforce to achieve security goals and attain and sustain adequate operational resiliency.
Awareness and Outreach	Provide wide-reaching communication on the importance of security and operational resiliency to the internal and external stakeholders of the enterprise.

Technology Assets and Infrastructure

The capability area of Technology Assets and Infrastructure highlights the importance and pervasive use of technology to support organizational business processes and the achievement of goals. Processes in this area focus on the security and resiliency of the organization's technology infrastructure and related assets across their entire life cycle—from development and implementation to operation and retirement. The contribution of systematic and disciplined IT operations and service management to security and operational resiliency is highlighted.

Table 5 describes proposed capabilities for the Technology Assets and Infrastructure capability area.

Table 5: Technology Assets and Infrastructure capabilities

Capability	Short Description
Technology Asset[27] Management	Identify, document, and manage technology objects that support critical business processes and contribute to achieving security goals and attaining and sustaining operational resiliency.
IT Infrastructure Management	Manage the operational information technology infrastructure to satisfy security goals and operational resiliency requirements.
Software and Systems Resiliency Management	Consider security and resiliency requirements early in the life cycle of software and systems that are developed or acquired and integrated by the enterprise to support mission-critical business processes.

[26] *Workforce* in this context refers to personnel whose primary role in the organization is to provide security and directly related operational resiliency services (such as business continuity planners).

[27] *Technology asset* refers to any technology object that supports the operation of a business process, including hardware, software, networks and telecommunications links, and personal computers.

Information and Data

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 in 2004 the estimated ratio of market capitalization in organizations had exploded to 15% tangible assets to 85% intangible assets [Anders 04]. This data 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 capital—to ensure that it is available in the form intended for use in business processes—is the focus of the Information and Data capability area. Processes included in this capability area address the organization's ability to inventory, value, protect, and communicate information with a focus on the connection between information assets and the underlying business processes and application systems that rely on them.

Table 6 describes the proposed capability for the Information and Data capability area.

Table 6: Information and Data capability

Capability	Short Description
Information Asset[28] Management	Identify, document, and manage information assets to ensure their availability for use by critical business processes.

Physical Plant

The physical plant of the organization forms another vital category of assets that the organization needs to accomplish its mission. The buildings where people work, where products are developed and produced, and where vital assets are stored and maintained are all integral to the organization's ability to execute critical business processes. The Physical Plant capability area represents processes necessary to inventory physical plant assets, addressing their security and resiliency by examining their purpose and ensuring that their role in the resilient organization is considered and planned for.

Table 7 describes proposed capabilities for the Physical Plant capability area.

[28] *Information asset* is any information or data that is important to the enterprise in the pursuit of its mission. Examples include intellectual property, employee records, and vendor databases. Information assets are often referred to as *vital records* in the business continuity discipline.

Table 7: Physical Plant capabilities

Capability	Short Description
Resiliency Facility[29] Management	Identify and manage resiliency-focused physical plant assets to ensure their availability for use by critical business processes during a disruptive event.
Enterprise Facility[30] Management	Identify and manage enterprise physical plant assets to ensure their availability for use by critical business processes.

Resiliency Relationships

No organization exists without vital external connections. Both upstream and downstream, organizational relationships with external partners are essential to accomplish goals. Capabilities in this area represent processes that are focused on ensuring that the security of the organization is not undermined as a result of exposure to external environments. In addition, processes address the need to consider operational resiliency for business processes as it extends to all external business partners—the resiliency value chain. Capabilities in this area focus not only on those partners who provide essential business services but also those that provide vital security services and directly help the organization to ensure business continuity and resiliency.

Table 8 describes proposed capabilities for the Resiliency Relationships capability area.

Table 8: Resiliency Relationships capabilities

Capability	Short Description
Internal Partnerships	Establish and manage an active relationship between business units and resiliency service providers to ensure resiliency of critical business processes.
Business Partner Management	Identify and manage resiliency relationships with upstream business partners to ensure end-to-end operational resiliency.
Stakeholder Relationship Management	Identify and manage relationships with customers and stakeholders that could be affected by changes in operational resiliency.
Service Partner Management	Identify and manage relationships with business partners who are directly involved in providing services that assist the enterprise in achieving security goals and attaining and sustaining an adequate level of operational resiliency.
Public Authority[31] Relationship Management	Identify and manage relationships with local and geographical authorities to coordinate planning and response to disruptive events in the environment in which the enterprise operates.

[29] A *resiliency facility* is a facility that has the specific purpose of supporting the organization if it is affected by a disruptive event. A backup data center is one example. A resiliency facility may or may not be owned directly by the organization. It may be stand-alone or may be shared with other operational functions.

[30] An *enterprise facility* is all organizational real estate and physical plant that is *not* directly involved in providing resiliency services during a disruptive event. This may include office buildings, power plants, and maintenance facilities that are used in day-to-day operations.

[31] A *public authority* is described as government and other related agencies that provide citizen services under legal or other arrangements. Public authorities include police and fire departments, emergency responder agencies, and public communications.

Table 8, cont.: Resiliency Relationships capabilities

Contract Management	Consider and support security and operational resiliency standards and requirements in the execution of contracts with third parties.
Logistics Management	Plan and document the activities necessary to ensure the movement of resiliency objects to support mission-critical business processes during a disruptive event.

Service Delivery

Service Delivery addresses the processes that the organization must perform in order to provide security and business continuity services to the enterprise. These capabilities represent several core activities, including business continuity planning, incident management, and crisis management.

Table 9 describes proposed capabilities for the Service Delivery capability area.

Table 9: Service Delivery capabilities

Capability	Short Description
Support Technology	Identify and deploy technologies that support the enterprise in delivering security and operational resiliency services.
Continuity Planning	Develop and deploy plans to ensure the continuity of mission-critical business processes.
Continuity Plan Validation	Systematically test and revise continuity plans to ensure that they meet their objectives for sustaining continuity of mission-critical business processes.
Recovery Planning	Develop and deploy plans to ensure the adequate recovery of security and resiliency objects that support mission-critical business processes under disruptive operating circumstances.
Restoration Planning	Develop and deploy plans to ensure the full restoration of mission-critical business processes to a predefined operating state.
Communications	Establish processes for communicating between service providers and external stakeholders before, during, and after disruptive events.
Event Identification and Analysis	Establish processes to identify and analyze events to determine an appropriate course of action for the enterprise and its business partners.
Crisis Management	Develop and deploy plans to manage activities that focus on disruptive events that post critical impact to enterprise operations.

Resiliency Sustainment

In addition to business processes, organizations need to manage the processes that directly and indirectly address the security and resiliency of the organization's operations. Capabilities in the Resiliency Sustainment area are focused on ensuring that the organization's process improvement approach to security and resiliency contributes to its ability to attain and sustain an adequate level of operational resiliency commensurate with organizational drivers.

Table 10 describes proposed capabilities for the Resiliency Sustainment capability area.

Table 10: Resiliency Sustainment capabilities

Capability	Short Description
Intergroup Coordination	Recognize and address interrelationships, interdependencies, and conflicts in security and resiliency planning and service delivery.
Process Management	Sustain and improve the enterprise security and operational resiliency processes through active process management and measurement.
Quality Assurance	Periodically review and audit the results of the security and operational resiliency management process and ensure that it is meeting requirements and goals.
Services Definition	Develop, maintain, and communicate an inventory of security and operational resiliency services provided by the enterprise.

6 Collaborating with the Banking and Finance Industry

Finding practical examples of organizations or industries that are making progress in the fields of security and business continuity through focusing on operational resiliency is challenging. The concepts of organizational and operational resiliency are still too abstract for many organizations. In addition, viewing activities like security and business continuity as enterprise-wide processes that can be defined, managed, and improved is in direct conflict with decades-old business models. However, by necessity organizations in the banking and finance industry have often exhibited operational maturity because of the complexity of their operations and their critical role in supporting the global economic infrastructure. In essence, a financial institution cannot fail without ripple effects being felt throughout the industry and the economy. Because of this, financial institutions are a perfect proving ground for evolutionary approaches like those described in this technical note. They support the exploration and development of a process improvement approach to operational resiliency because their organizational drivers demand it.

6.1 Critical Infrastructure Protection

For the U.S.-based financial services industry, the events of September 11, 2001, and their aftermath broke a number of previously held assumptions about likely and unlikely threats. The effect of extensive infrastructure damage on a highly interconnected, interdependent "business ecosystem" was a shocking wake-up call. And the catalog of catastrophic disruptions continues to grow. Massive power outages on both coasts, powerful and devastating hurricanes that impact entire cities and damage critical industries, and a proliferation of cyber attacks that strike key networks and computer systems have all contributed to a heightened sense of vulnerability and underscored the need for sophisticated and measurable protection.

Banks and financial institutions have always been on the forefront of security and business continuity management. But today there is unprecedented pressure to manage risk and to be prepared to respond to business disruptions. This pressure is coming from regulators, customers, management, and most significantly from shareholders and equity markets.

The Interagency Whitepaper drafted jointly by a variety of key federal regulatory agencies has been the most notable and controversial driver for change in the financial sector [SEC 02]. While this document targeted the financial sector, it has had significant influence on virtually all businesses because it set the tone for the ongoing dialogue on what should be done to strengthen operational risk management, particularly in the area of business continuity. The Securities and Exchange Commission outlined the mandate as follows:

> On September 5, 2002, the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and the Securities and Exchange Commission published for comment a Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System. The draft white paper emphasized the criticality of protecting the financial system from serious new risks posed in the post-September 11 environment and described a series of sound practices that were identified by industry participants during a series of interviews and meetings with the agencies [SEC 02].

The heightened sense of vulnerability has led the federal government to redefine the term "critical infrastructure" for the country. For many years the nation's critical infrastructure was simply defined as the adequacy of the nation's public works (e.g., water, electricity). The USA PATRIOT Act of 2001[32] vastly changed the definition of critical infrastructure to describe systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national economic security, national public health and safety, or any combination of those matters [PATRIOT 01].

Due to the overall raised consciousness around critical infrastructure protection, customers and shareholders increasingly expect institutions to be resilient and to demonstrate their resiliency. It is no longer acceptable for organizations to be complacent in measuring and communicating the effectiveness of their risk management activities. A process view of operational resiliency provides the impetus for the industry to begin defining what can be measured and to actually measure it on a regular basis. It will allow organizations to identify gaps and then communicate to their stakeholders how they will fill those gaps.

A study published by Templeton College of Oxford University that focused on the impact of catastrophes on shareholder value noted that firms affected by catastrophes fall into two relatively distinct groups: recoverers and non-recoverers [Knight 96]. While all catastrophes have an initial negative impact on value, they also offer an opportunity to management to demonstrate their talent in dealing with difficult circumstances. Firms that fell into the category of recoverers increased shareholder value; in organizations categorized as non-recoverers, shareholder value fell significantly.

Embracing a process improvement framework for security and resiliency enables the industry to demonstrate to its stakeholders that it recognizes the need to sustain and improve operational resiliency and to communicate to the market its relative ability to do so.

[32] The introduction and passage of the USA PATRIOT Act of 2001 was a direct result of the events of September 11, 2001.

6.2 Movement Toward Process Improvement

Put simply, banking and financial institutions need to know how well they are performing in meeting their operational resiliency goals. They need to be able to predict, to the extent possible, how they will fare when the next disruptive event comes. But today they have no consistent way to do this. In an industry where there is so much interlinking, the fact remains that each institution is probably using a different scale (if any at all) to determine how capable it is.

Banking and financial institutions often do not have complete control over achieving the goals of a business process. Success is a collaborative effort of internal and external partnerships—a value chain aimed at common goals. A primary driver for embracing a process improvement approach is the ability to determine consistently and objectively where the weakest links are in this chain, far in advance of discovering this during a disruptive event. A business partner that does not embrace resiliency to the same degree as the organization can be identified and replaced. In this way, banking and finance institutions give themselves more control over a situation they inherit as part and parcel of their complex, interconnected industry.

A secondary driver is the ability to develop and deploy a common taxonomy. The language of security, business continuity, and now resiliency has emerged through various perspectives and applications and is now almost too unwieldy to make productive use of. The development of a process improvement framework to date has forced normalization of this language so that process definitions are accurate, consistent, and understandable. In the future, the common language of operational resiliency may help banking and financial institutions to improve communication and collaboration, making their interdependencies more manageable. (More information on a taxonomy for operational resiliency is included in Appendix A.)

6.3 Driving Out Cost and Improving Value

As in all industries, organizations are pressured by stakeholders and other constituencies to improve value at the lowest possible cost. In an industry like banking and finance that is looking for growth opportunities, internal process improvement is one way to improve cost structures and fuel future opportunities. Unfortunately, activities like security and business continuity are expensive and, because they are often not well managed, tend to take a larger share of expense budgets for the return they bring to the organization. But by defining standard processes and having the capability to measure and improve them, financial institutions might be able to realize cost savings and increases in overall effectiveness.

6.4 Managing Regulatory Compliance

The banking and finance industry is one of the most highly regulated industries in the world. Since it is such a critical component of the world's economic infrastructure, governments have a significant interest in ensuring that its institutions remain stable. Regulations and best practices are created in an attempt to ensure some minimal level of performance. One of the consequences of this regulatory environment is that organizations can lose focus on managing their

operational risks and instead become solely focused on compliance. While being compliant with regulations is certainly a critical success factor for a financial institution, it should not be the sole focus when security, continuity, or IT operations decisions are being made.

The Interagency Whitepaper clearly acknowledges that overall recovery requires cooperative action to be successful: "The events of September 11 underscored the fact that the financial system operates as a network of interrelated markets and participants. The ability of an individual participant to function can have wide-ranging effects beyond its immediate counterparties. Because of the interdependent nature of the U.S. financial markets, all financial firms have a role in improving the overall resilience of the financial system" [SEC 02]. The financial sector's recognition of the need to work together is facilitated by the development of a resiliency model and the related taxonomy of terms.

A framework that allows an organization to determine its capacity to manage operational resiliency and to determine the level of resiliency necessary for its unique operating circumstances can translate into more effective risk management strategies, avoidance of wasted resources and high-risk environments, and unnecessary regulation. To the extent that regulators are able to use such a framework to ensure that banking and financial institutions are competent in managing operational resiliency, less prescriptive regulatory guidance may result.

The Interagency Whitepaper mandates the financial sector to be more proactive in finding ways to improve their recoverability and resiliency. "The agencies believe that it is important for financial firms to improve recovery capabilities to address the continuing, serious risks to the U.S. financial system posed by the post-September 11 environment" [SEC 02]. An operational resiliency framework provides not only a means to demonstrate compliance with the direction set by regulators, but it provides a valuable tool for improving the process and eventually delivering compliance as a byproduct of good process management.

6.5 Starting from a High-Performing Perspective

Managing operational resiliency is about managing operational risk. Because of their transactional complexity, banks and financial institutions have realized this fact long before regulators have called for action. Each day trillions of dollars in financial transactions flow through the interconnected electronic networks of the world's banks and financial institutions. Timeliness and reliability are operational requirements for these transactions, as are the high availability and integrity of the industry's operational infrastructure. Being able to operate without interruption is critical to the profitability of these organizations and the stability of the world's economy. As a critical element in the global economic infrastructure, the banking and finance industry has a substantial history of sophisticated operational risk management and contingency planning capabilities.

The tie to the stability of world economies has resulted in the creation of many high-performing organizations in the banking and finance industry. Operational resiliency is a way of life for many of these organizations because of the important functions they perform. Con-

sider the Depository Trust and Clearing Corporation (DTCC). Through its subsidiaries, it provides clearance, settlement, and information services for equities, corporate and municipal bonds, government- and mortgage-backed securities, and over-the-counter credit derivatives. Inability to perform these functions affects the safety and soundness of financial markets. Or consider the operation of the computer systems and communication networks that support the New York Stock Exchange® (NYSE®) and the American Stock Exchange® (AMEX®). The Security Industry Automation Corporation (SIAC) is responsible for the design, development, and management of these systems and networks. For these organizations, operational resiliency is an explicit requirement of their core mission, and therefore they lead the way in practical implementation of many of the concepts discussed in this report. Operational resiliency is not a theory for them; it is how they do business.

The ubiquitous use of technology by companies in the banking and finance industry is also a driver for their early adoption of process improvement techniques. Many of FSTC's member companies are users of CMMI and other process improvement models, and some are using techniques like Six Sigma to drive down costs and improve effectiveness. This provides a foundational and important analog for viewing security and business continuity as processes and for adoption of process improvement techniques to improve operational resiliency.

6.6 Moving Forward Together

The nature of banking and finance organizations makes them a perfect partner for exploring process improvement for operational resiliency. They recognize the benefits of structured approaches to process management, the definition and application of common standards and taxonomy, and the importance of having a consistent and credible tool for assessing their operational resiliency competency. They are comfortable with process improvement and often have well-defined capabilities on which to build. They support a process improvement approach because it provides them with the tools they need to continue to drive down costs and improve value to shareholders. And finally, they "live" operational resiliency on a daily basis, and thus are uniquely capable and experienced in defining and developing a framework for process improvement.

7 Future Research and Direction

Much work has been done over the past two years in framing and scoping the basic activities that we feel are necessary to perform security across an organization with an eye toward operational resiliency, but much work remains to be done. In this section we describe our future research plans to continue progress toward a process improvement framework.

7.1 Next Steps

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

- Identify and publish a first level of the framework.
- Continue collaboration with FSTC.
- Begin exploration with the SEI CMMI program.
- Explore the maturity aspects of the framework.
- Explore the metrics and measurement aspects of the framework.
- Continue to research best practices and activities and map them against the framework.
- Obtain community input and direction.

Each of these activities is discussed in more detail below.

7.1.1 Identify and publish a first level of the framework

Subsequent to the publication of this technical note, our focus turns to the development and publication of a draft process improvement framework for operational resiliency. This will allow us to accomplish several things. First, it will capture our current thinking on the structure of the framework and the set of capabilities it contains. Second, publishing this information will provide a vehicle for community feedback on the direction of this work and subsequent iterations of the framework.

7.1.2 Continue collaboration with FSTC

Collaborating with FSTC and the organizations that are participating in FSTC's Resiliency Model Project has been invaluable to our work. Most of the participants in this FSTC project are very large banks and large consulting firms and most have experience with process improvement models of one kind or another. In fact a significant number have direct experience with CMMI. In addition, due to the nature of their business, they have a deep understanding of operational risk management.

The FSTC-sponsored workshops planned in the coming year will continue to provide us with a forum to draw on the experience and expertise of the project participants, especially in the areas of business continuity, disaster recovery, and IT operations. Access to this expertise ensures that the capabilities we identify are robust and reflective of what is being done in practice.

7.1.3 Collaboration with SEI CMMI Initiative

For more than 20 years, the SEI has worked to advance the state of the practice of software engineering and to serve as a national resource in software engineering and technology. Beginning with the introduction of the SW-CMM in 1987 and continuing today with CMMI, the SEI has a successful history of developing process improvement models that have been proven to be effective and have broad acceptance in the community. In addition to creating the frameworks, the SEI has created infrastructures that ensure the support and development of these models going forward.

We believe that the unique combination of our experience in information security and the CMMI Initiative's experience in developing and supporting improvement frameworks makes the SEI the ideal environment for the development of a framework for operational resiliency. However, this does not necessarily mean that the framework will be integrated into the CMMI Product Suite. A framework for operational resiliency is certainly different in scope than those focused on the software and systems development processes, but there may be valid and important connections. This remains an area of continuing research that must be explored as our work evolves.

7.1.4 Explore maturity aspects of the framework

Certainly one of the most important requirements for the banking and finance community is to be able to use the process improvement framework as a means for identifying their target and setting upon an improvement course. However, there is also a strong requirement for being able to "rate" organizations as to their process maturity for managing operational resiliency, particularly when the framework is applied to the bank's upstream and downstream business partners. Through our initial phases of work, we have found anecdotal evidence of process maturity, but have not been able to validate this. Thus, this is an area of research that needs further exploration, and we will be mindful of such requirements as we continue development.

7.1.5 Explore metrics and measurement aspects of the framework

Identification of meaningful metrics and appropriate measurements is a fundamental aspect of process improvement. Unfortunately, in the areas of security and business continuity, meaningful metrics are often difficult to identify and measure. Our aim in the development of the framework is to analyze and develop metrics that would help organizations to measure their progress in managing the operational resiliency process across a number of key capabilities, all of which contribute to meeting resiliency goals. In addition, appropriate metrics can also substantiate the business case for investing in the implementation and management of a process

improvement approach to resiliency. This is particularly important to the banking and financial community in that the investment in process management must reap tangible returns to the organization in terms of improved deployment of resources to protect and sustain critical assets.

7.1.6 Continue to research best practices

Another objective as we move forward is to identify and map best practices and activities to the framework. As part of the research in identifying an initial set of capabilities, we created affinity groupings using a number of information security and operations best practices. In this next stage of development we will be using a more diverse set of best practices and activities and will be attempting to map practices to capabilities this time instead of grouping practices to find capabilities. This will allow us to identify possible gaps in the current framework and for activities that reflect common practices to be assigned to the capabilities. It will also have the added benefit of allowing users of the framework to understand how the adoption of these best practices helps them achieve capabilities in their organizations.

In order to do this we must first identify which practices to include in the mapping exercise. We expect these to come from our interactions with FSTC and the community of interest that we develop around this work. The boundaries on which practices to include and which to exclude will ultimately depend on how we answer the question of whether a boundary exists between a process improvement framework for security management and for operational resilience.

7.1.7 Obtain community input and direction

In addition to the activities described above, we believe that developing a community of interest around this work is vital to its success. For this model to be accepted and achieve its intended results, we will need significant input from the community. Our collaboration with FSTC and its member organizations has been a significant factor in the success of this project to date. In the coming year we intend to seek out other similar organizations to partner with us to further this work.

Once we have stabilized an initial version of the framework, we intend to create a questionnaire based on the framework and distribute it to members of the FSTC project. We will also seek other members of the community for a similar effort. The questionnaire will allow us to gauge the current state of the practice and provide us more information on the possible maturity and process improvement aspects of our model. In addition, we hope that feedback generated from the questionnaire will provide additional information for the refinement of the model.

In addition to the planned publications and questionnaire, we plan to continue our exposition of this work in public forums and conferences. We will seek out other opportunities throughout the coming year to continue to publicize this work and to obtain feedback.

7.2 Feedback on this Technical Note

The publication of this technical note is a first step in introducing a process improvement framework for security management to the community. Readers of this technical note are encouraged to explore and discuss the concepts we introduced. We also welcome readers to share their comments and suggestions and descriptions of their experiences with the framework. All feedback can be directed to our project mailbox, esm-info@cert.org.

8 Conclusions

The importance of managing operational risk will continue to grow as the operational and technical environment of today's organization expands. The emphasis on cutting costs, improving productivity, and gaining a competitive edge requires that organizations use all of their competencies to support organizational drivers and propel them toward their missions. Activities like security, business continuity, and IT operations management must be active contributors to this effort. But current approaches to managing these activities as separate, disconnected approaches to support will continue to be a drag on organizations' limited resources and will not produce the intended effect—to support and sustain operational resiliency.

The convergence of these activities is not just a foundation of our theories and assertions but is a natural outgrowth of the risk management connection between these activities. But convergence requires collaboration, and organizations will need to overcome deeply ingrained cultural and funding barriers to guarantee it. We see the introduction of a process approach—led by security management—as a promising way for organizations to operationalize these theories and to actively direct and control operational resiliency.

Appendix A Emerging Taxonomy

A list of key terms and concepts used in the general field of operational resiliency has been developed as part of our collaboration with FSTC. It is intended as an emerging common reference, and its purpose is to foster standardization and communication among those working in the broad areas of disaster recovery, business continuity, and related fields, whether as practitioners, analysts, modelers, system builders, or policymakers. Because of the size of the taxonomy, we have not included it in this technical note. However, it can be viewed at http://www.fstc.org/projects/taxonomy.

It is intended that authors of documents, business processes, models, and software use the taxonomy as a means to standardize their terminology, making their work easier to understand, use, and maintain. As a side benefit, it may also be useful to those creating object models or other abstract representations of business processes.

The taxonomy was initially created by the Financial Services Technology Consortium during Phase I of the Resiliency Model Project. The terms and concepts it contains were drawn from a number of industry sources (described in Table 11), as well as from the original work of the project team.

Starting with the source materials, the creators of this taxonomy extracted approximately 4,700 terms likely to be of interest. Through a careful editing and comparison process, the team standardized spelling and phrasing, eliminated outright duplicates, identified and documented synonyms, and eliminated terms identified as being too specific or otherwise not of general interest. Where there was conflict between the definitions of a given term across two or more source documents, the editors resolved the conflict, keeping one term and deprecating the other. In each case, a link to the original term and the original source material has been preserved.

It is anticipated that further growth and development of a process improvement model will necessitate changes to this taxonomy as well as expansion to include relevant security and IT operations-related terminology.

Table 11: Taxonomy sources

Organization	Source Document	Reference	Abbreviation Used in Taxonomy
All Hands Community	Glossary	http://www.all-hands.net/pn/modules.php?op=modload&name=pn_glossary&file=index	All Hands
ASIS International	Glossary	http://www.asisonline.org/	ASIS
Business Continuity Institute	Glossary	http://www.thebci.org/Glossary.pdf	BCI
Business Roundtable	*CEO Guide to Security Challenges*	http://www.businessroundtable.org/pdf/20050503003CEORiskMgmtGuideFINAL.pdf	CEO Guide
DRI International and *Disaster Recovery Journal*	*Disaster Recovery Journal* Business Continuity Glossary	http://www.drj.com/glossary/drjglossary.html	DRII
IBM	Various	http://www-1.ibm.com/services/us/bcrs/html/resilience_library.html	IBM
TSO	ITIL glossary	http://www.get-best-practice.co.uk/glossary.aspx?product=ictinfrastructurelibrary	ITIL
Metavante	Internal document	N/A	Metavante
National Fire Protection Association	NFPA 1600 Standard	http://www.nfpa.org/PDF/nfpa1600.pdf?src=nfpa	N1600
National Fire Protection Association	Other NFPA documents	http://www.nfpa.org/assets/files/PDF/GlossaryA2004.pdf	NFPA

Appendix B Practice Sources

The following describes the primary sources of best practices that form the basis for our definition of a process view of operational resiliency. Additional sources continue to be referenced and will be fully identified and described in the publication of a process improvement framework.

BS7799/ISO17799

BS7799/ISO standard 17799 sets the requirements for an information security management system or process. It is intended to be used by organizations for the identification and management of the range of threats to which information is routinely subjected. The standard is organized into 10 coverage areas: security policy, organization of assets and resources, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance. For the ESM project, the BS/ISO standard provides valuable input from a security management perspective.

Further information on BS7799 and ISO standard 17799 can be found at http://www.bsi-global.com/ or http://www.iso.org/.

COBIT

COBIT loosely translates to "control objectives for information and related technology." It is issued by the IT Governance Institute (http://www.itgi.org/) and promoted by the Information Systems Audit and Control Association (http://www.isaca.org/). It has been developed as a general standard for information technology security and control practices and includes a general framework for management, users, IS audit, and security practitioners. COBIT also has a process focus and a governance flavor; that is, management's need to control and measure IT is a focus point. COBIT covers over 30 IT processes in four domains including planning and organization, acquiring and implementing, delivery and support, and monitoring. COBIT also includes a maturity model for IT processes to assist with capability improvement. The intersection between security and IT controls and governance as represented in COBIT is a major focus of the ESM project.

IT Infrastructure Library (ITIL)

The IT Infrastructure Library is a widely accepted collection of best practices for IT service management. It consists of a series of works focused on the delivery of quality IT services and on the environment in which IT operates. It focuses on the growing dependency of organizations on IT to satisfy their missions, which in turn requires high-quality, reliable IT processes.

ITIL is an important ingredient in the ESM work because IT service and operations excellence often translates to higher levels of security and contributes to resiliency. Thus, the inclusion of a model that focuses at the IT service (and service management) level provides another dimension of input to the ESM capabilities that is not directly focused on security yet provides security benefits.

More information on ITIL can be found at http://www.ogc.gov.uk/.

Information Security Forum (ISF)

The Information Security Forum is an international association of over 250 leading companies and public sector organizations that fund and cooperate in the development of practical research in information security. The ISF produces *The Standard of Good Practice for Information Security* (The Standard), which is based on 14 years of ongoing research and is positioned as an aid to organizations in understanding and applying best practices for information security. Because it addresses security from a business perspective, The Standard appropriately recognizes the intersection between organizational drivers and security drivers, and thus is a good fit for our work in enterprise security management.

Additional information on the ISF and The Standard can be found at http://www.securityforum.org/.

DRII Professional Practices for Business Continuity Planners

DRI International (DRII) was first formed in 1988 as the Disaster Recovery Institute in St. Louis, Missouri. A group of professionals from the industry and from Washington University in St. Louis forecast the need for comprehensive education in business continuity. Alliances with academia helped shape early research and curriculum development.

The group also understood that individual certification and establishing a common body of knowledge (standards) could only enhance industry professionalism. As a result, the new nonprofit organization established its goals to

- promote a base of common knowledge for the business continuity planning/disaster recovery industry through education, assistance, and publication of the standard resource base
- certify qualified individuals in the discipline
- promote the credibility and professionalism of certified individuals

DRII sets standards that provide the minimum acceptable level of measurable knowledge, thus providing a baseline for levels of knowledge and capabilities. Accordingly, in 1997, DRII, together with BCI, published the Professional Practices for Business Continuity Planners as the industry's international standard.

Additional information on DRII and the Professional Practices can be found at http://www.drii.org/.

Generally Accepted Business Continuity Practices

The DRJ Editorial Advisory Board (EAB) has created the Generally Accepted Practices (GAP) for the business continuity industry. The DRJ Generally Accepted Business Continuity Practices Committee has established 10 subcommittees of seasoned business continuity professionals from partner organizations and members from the public and private sectors. These committees have identified and documented standards and guidelines to create universally accepted business continuity practices in order to benefit the entire business continuity profession.

The mission of the DRJ-EAB effort is to have the GAP recognized as a leading source of sound practices. The practices are compiled in a depository of knowledge and expertise submitted by experienced business continuity practitioners. The DRJ has partnered with the following organizations to assist in the creation of the GAP:

- Association of Records Management Administration
- DRI International
- Financial Services Technology Consortium
- Standards Australia/Standards New Zealand
- National Fire Protection Association

The first draft of this highly anticipated document is currently available at http://www.drj.com/GAP/.

Other sources

In addition to the sources listed above, we are exploring other guidelines, standards, and practices for inclusion in our mapping exercise. Of note is the inclusion of regulatory guidelines such as HIPAA (particularly the security standards found at http://www.cms.hhs.gov /SecurityStandard/). These guidelines are important because organizations must exhibit security management capabilities that permit them to meet the compliance standards as well as to manage their compliance activities.

Another source of relevant practices is the National Institute of Standards and Technology (NIST) 800-level series on information security. In particular, we are concentrating on NIST

800-14, *Generally Accepted Practices and Principles for Securing Information Systems* (http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf). As we use this information in our work with federal government civilian agencies, we continue to be aware of its influence on the security management processes in organizations, and thus will include relevant NIST 800 documents as necessary.

Appendix C FSTC Collaborators

Table 12 provides a list of members of the Financial Services Technology Consortium who have participated in our Phase I exploratory activities. We are sincerely grateful for their input and contributions and look forward to future collaboration.

Table 12: List of FSTC collaborators

Organization	Participant	Title/Department
Ameriprise Financial http://www.ameriprise.com/	Barry Gorelick	Vice President, Ameriprise Business Continuity Management
Bank of America http://www.bankofamerica.com/	Andrew McCruden	Senior Vice President, Corporate Business Continuity
	Sara Ricci	Corporate Business Continuity
	Deborah Sanders	Senior Vice President, Corporate Business Continuity
	Tina Speiss	GCIB Business Continuity
	Barbara Spradling	Corporate Business Continuity Executive
Capital Group http://www.capgroup.com/	Michael Gifford	Manager, Disaster Recovery
Citigroup http://www.citi.com/	Gregory Gist	Vice President, Office of Business Continuity
Discover Financial http://www.discoverfinancial.com/	Rick Webb	Technology Risk Management
	Kent Anderson	Technology Risk Management
DRI International http://www.drii.org/	John Copenhaver	Chief Executive Officer
Disaster Recovery Journal http://www.drj.com/	Richard Arnold	President
Federal Reserve Bank of New York http://www.ny.frb.org/	Todd Waszkelewicz	Supervisory Officer

Organization	Participant	Title/Department
Financial Services Technology Consortium http://www.fstc.org/	Jim Salters	Director, Technical Initiatives and Project Development
	Zach Tumin	Executive Director
	Charles Wallen	Managing Executive, Business Continuity
IBM http://www.ibm.com/	Richard Cocchiara	Executive Consultant, CTO Business Resilience
	Damian Walch	Consulting Practice Lead
Interisle Consulting http://www.interisle.net/	Chris Owens	Principal Consultant
	Colin Strutt	Principal Consultant
JPMorganChase http://www.jpmorganchase.com/	Lynn Houseknecht	Managing Director, Global Technology Infrastructure, Risk Management
	Rich Magro	Managing Director, Resiliency Risk Management
	Judith Zosh	Vice President, Global Technology Infrastructure, Business Resiliency
Key Bank http://www.key.com/	Shelly Christensen	Corporate Continuity and Recovery
	Pat Metz	Corporate Continuity and Recovery
	Don Culp	Corporate Continuity and Recovery
	Deborah Minch	Corporate Continuity and Recovery
	Lisa Swiney	Corporate Continuity and Recovery
	Charlene Whitcomb	Manager, Corporate Continuity and Recovery
KPMG http://www.us.kpmg.com/	Jeff Dato	Senior Manager, Advisory Services Security, Privacy and Continuity
	Cole Emerson	Director, Advisory Services Security, Privacy and Continuity
	Marty Plevel	Senior Manager, Advisory Services Security, Privacy and Continuity

Organization	Participant	Title/Department
Marshall & Ilsley http://www.mibank.com/	Gary Daniels	Vice President, Corporate Business Continuity Planning
	Matt Meyer	Corporate Business Continuity Planning
	Beth Nickerbocker	Chief Risk Officer
MasterCard http://www.mastercardinternational.com/	Randall Till	Senior Business Leader, Global Business Continuity Management
SunGard http://www.sungard.com/	Chris Burgher	Engagement Manager, Information Security Professional Services
	John Sensenich	Director, Product Management and Development
US Bank http://www.usbank.com/	Thomas Hirsch	Senior Vice President
	Jeffrey Pinckard	Business Recovery Manager
	Michael Rattigan	Director, Business Continuity
	Mick Stickney	Business Continuity Manager
Wachovia http://www.wachovia.com/	Brian Clodfelter	Continuity Testing Oversight
	Sam Handsman	Technology Recovery Manager
	Pat Rosa	Business Continuity Manager

References

URLs are valid as of the publication date of this document.

[Anders 04] Anders, Donald E. "Attention ABLs…Are you Undervaluing Your Borrower's Greatest Assets?" *ABF Journal 2*, 7 (July/August 2004). http://www.accuval.net/insights/abf_journal.pdf.

[Caralli 04a] 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 04b] Caralli, Richard A. *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-2004-TR-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications/documents/04.reports/04tr010.html.

[CISWG 04] Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. "Information Security Management References." March 18, 2004. http://reform.house.gov/UploadedFiles/Best Practices Bibliography.pdf.

[Ellison 97] Ellison, B.; Fisher, D. A.; Linger, R. C.; Lipson, H. F.; Longstaff, T.; & Mead, N. R. *Survivable Network Systems: An Emerging Discipline* (CMU/SEI-97-TR-013, ADA341963). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. http://www.sei.cmu.edu/publications/documents/97.reports/97tr013/97tr013abstract.html.

[Fisher 00] Fisher, David A. & Lipson, Howard F. "Survivability—A New Technical and Business Perspective on Security." CERT Coordination Center, Software Engineering Institute, 2000. http://www.cert.org/archive/pdf/busperspec.pdf.

[Hamel 03] Hamel, Gary & Valinkangas, Liisa. "The Quest for Resilience." *Harvard Business Review 81*, 9 (September 2003). http://www.hbr.org/.

[Knight 96] Knight, Rory F. & Pretty, Deborah J. *The Impact of Catastrophes on Shareholder Value*. The Oxford Executive Research Briefings. Oxford, England: Templeton College, University of Oxford, 1996.

[PATRIOT 01] H. R. 3162, USA PATRIOT Act of 2001. http://www.fincen.gov/hr3162.pdf (2001).

[Riskglossary 06a] riskglossary.com. *Basel Committee on Banking Supervision*. http://www.riskglossary.com/articles/basle_committee.htm (2006).

[Riskglossary 06b] riskglossary.com. *Operational Risk*. http://www.riskglossary.com/articles/operational_risk.htm (2006).

[SEC 02] Securities and Exchange Commission. *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*. http://www.sec.gov/news/studies/34-47638.htm (2003).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	March 2006	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Sustaining Operational Resiliency: A Process Improvement Approach to Security Management	FA8721-05-C-0003

6. AUTHOR(S)

Richard A. Caralli

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-TN-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	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Organizations face an ever-changing risk environment. The risk that emanates from the day-to-day activities of the organization, operational risk, is the subject of increasing attention, particularly in the banking and finance industry, because of the potential to significantly disrupt an organization's pursuit of its mission. Security, business continuity, and IT operations management are activities that traditionally support operational risk management. But collectively, they also converge to improve the operational resiliency of the organization—the ability to adapt to a changing operational risk environment as necessary. Coordinating these efforts to sustain operational resiliency requires a process-oriented approach that can be defined, measured, and actively managed. This report describes the fundamental elements and benefits of a process approach to security and operational resiliency and provides a notional view of a framework for process improvement.

14. SUBJECT TERMS	15. NUMBER OF PAGES
enterprise security management, strategic planning, information security, risk management, operational resiliency	82

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