CERT Resilience Management Model, Version 1.0

Article · May 2010

CITATIONS
19

READS
973

5 authors, including:

Julia H Allen
Axio Global
52 PUBLICATIONS **1,390** CITATIONS
SEE PROFILE

Lisa Young
Carnegie Mellon University
11 PUBLICATIONS **310** CITATIONS
SEE PROFILE

Software Engineering Institute

CERT® Resilience Management Model, Version 1.0

Improving Operational Resilience Processes

Richard A. Caralli
Julia H. Allen
Pamela D. Curtis
David W. White
Lisa R. Young

May 2010

TECHNICAL REPORT
CMU/SEI-2010-TR-012
ESC-TR-2010-012

CERT Program

http:// www.cert.org/resilience/

Carnegie Mellon

This report was prepared for the

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

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

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

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

Table of Contents

List of Figures

List of Tables

Preface

The CERT® Resilience Management Model (CERT®-RMM) is an innovative and transformative way to approach the challenge of managing operational resilience in complex, risk-evolving environments. It is the result of years of research into the ways that organizations manage the security and survivability of the assets that ensure mission success: people, information, technology, and facilities. It incorporates concepts from an established process improvement community to create a model that transcends mere practice implementation and compliance—one that can be used to mature an organization's capabilities and improve predictability and success in sustaining operations whenever disruption occurs.

The ability to manage operational resilience at a level that supports mission success is the focus of CERT-RMM. By improving operational resilience management processes, the organization in turn improves the mission assurance of high-value services. The success of high-value services in meeting their missions consistently over time and in particular when stressful conditions occur is vital to meeting organizational goals and objectives.

Purpose

CERT-RMM v1.0 is a capability-focused process improvement model that comprehensively reflects best practices from industry and government for managing operational resilience across the disciplines of security management, business continuity management, and IT operations management. Through CERT-RMM these best practices are integrated into a single model that provides an organization a transformative path from a silo-driven approach for managing operational risk to one that is focused on achieving resilience management goals and supporting the organization's strategic direction.

CERT-RMM incorporates many proven concepts and approaches from the Software Engineering Institute's (SEI) process improvement experience in software and systems engineering and acquisition. Foundational concepts from Capability Maturity Model Integration (CMMI) are integrated into CERT-RMM to elevate operational resilience management to a process approach and to provide an evolutionary path for improving capability. Practices in the model focus on improving the organization's management of key operational resilience processes. The effect of this improvement is realized through improving the ability of high-value services to meet their mission consistently and with high quality, particularly in times of stress.

It should be noted that CERT-RMM is not based on the CMMI Model Foundation (CMF), which is a set of model components that are common to all CMMI models and constellations. In addition, CERT-RMM does not form an additional CMMI constellation or directly intersect with existing constellations. However, CERT-RMM makes use of several CMMI components, including core process areas and process areas from CMMI-DEV. It incorporates the generic goals and practices of CMMI models, and it expands the resilience concept for services found in CMMI-SVC. Section 1.4 of this report provides a detailed explanation of the connections between CERT-RMM and the CMMI models.

Acknowledgements

This report is the culmination of many years of hard work by many people dedicated to the belief that security and continuity management processes can be improved and operational resilience can be actively directed, controlled, and measured. These people have spent countless hours poring over codes of practice, interviewing senior personnel in organizations with high-performance resilience programs, applying and field testing the concepts in this report, and codifying the 26 most common process areas that compose a convergent view of operational resilience.

Early models were created by Richard Caralli working with members of the Financial Services Technology Consortium from 2004 through 2008. The model was significantly enhanced as additional model team members joined our efforts. The resulting model, CERT-RMM v1.0, is the work of the CERT-RMM Model Team, which includes Richard Caralli, David White, Julia Allen, Lisa Young, and Pamela Curtis.

CERT-RMM v1.0 was refined and recalibrated through benchmarking activities performed over a period of two years by security and continuity professionals at prominent financial institutions. The model team is forever indebted to the following people who participated in that effort.

- Ameriprise Financial: Barry Gorelick
- Capital Group: Michael Gifford and Bo Trowbridge
- Citi: Andrew McCruden, Patrick Keenan, Victor Zhu, and Joan Land
- Discover Financial Services: Rick Webb, Kent Anderson, Kevin Novak, and Ric Robinson
- JPMorgan Chase & Co.: Judith Zosh, Greg Pinchbeck, and Kathryn Wakeman
- Marshall & Ilsley Corporation: Gary Daniels and Matthew Meyer
- MasterCard Worldwide: Randall Till
- PNC Financial Services: Jeffery Gerlach and Louise Hritz
- U.S. Bank: Jeff Pinckard, Mike Rattigan, Michael Stickney, and Nancy Hofer
- Wachovia: Brian Clodfelter

In addition, we are grateful for the contributions of personnel from organizations who bravely performed early appraisal pilots using the model, including Johnny E. Davis; Kimberly A. Farmer; William Gill; Mark Hubbard; Walter Dove; Leonard Chertoff; Deb Singer; Deborah Williams; Bill Sabbagh; Jody Zeugner; Tim Thorpe and the many other participants from the United States Environmental Protection Agency; and Nader Mehravari, Joan Weszka, Michael Freeman, Doug Stopper, Eric Jones, and many other talented people from Lockheed Martin Corporation.

Last, but certainly not least, we owe much of the momentum that created this model to Charles Wallen from American Express. In 2005, as the executive director of the Business Continuity Standing Committee for the Financial Services Technology Consortium, Charles came to the CERT Program at the Software Engineering Institute with a desire to create a resiliency maturity model based on work being performed at CERT. Five years later we have a functional model (which is only four years and 46 weeks longer than we hoped it would take!).

We would also like to thank those who supported this effort at the Software Engineering Institute and CERT.

We thank Rich Pethia, director – CERT Program, for his support, patience, encouragement, and direction during the development and piloting of the model. We have special thanks for William Wilson, deputy director – CERT Program, and Barbara Laswell, director – CERT Enterprise Workforce Development Directorate, for their day-to-day direction and assistance in helping us build a community of believers and helping us navigate our way through all of the challenges inherent in a long, arduous effort.

Audience

The audience for CERT-RMM is anyone interested in improving the mission assurance of high-value services through improving operational resilience processes. Simply stated, CERT-RMM can help improve the ability of an organization to meet its commitments and objectives with consistency and predictability in the face of changing risk environments and potential disruptions. CERT-RMM will be useful to you if you manage a large enterprise or organizational unit, are responsible for security or business continuity activities, manage large-scale IT operations, or help others to improve their operational resilience. CERT-RMM is also useful for anyone who wants to add a process improvement dimension or who wants to make more efficient and effective use of their installed base of codes of practice such as ISO 27000, COBIT, or ITIL.

If you are a member of an established process improvement community, particularly one centered on CMMI models, CERT-RMM can provide an opportunity to extend your process improvement knowledge to the operations phase of the asset life cycle. Thus, process improvement need not end when an asset is put into production—it can instead continue until the asset is retired.

Organization of This Document

This document is organized into three main parts:

- Part One: About the CERT Resilience Management Model
- Part Two: Process Institutionalization and Improvement
- Part Three: CERT-RMM Process Areas

Part One, About the CERT Resilience Management Model, consists of four chapters:

- Chapter 1, Introduction, provides a summary view of the advantages and influences of a process improvement approach and capability maturity models on CERT-RMM.
- Chapter 2, Understanding Key Concepts in CERT-RMM, describes all the model conventions used in CERT-RMM process areas and how they are assembled into the model.
- Chapter 3, Model Components, addresses the core operational risk and resilience management principles on which the model is constructed.
- Chapter 4, Model Relationships, describes the model in two virtual views to ease adoption and usability.

Part Two, Process Institutionalization and Improvement, focuses on the capability dimension of the model and its importance in establishing a foundation on which operational resilience management processes can be sustained in complex environments and evolving risk landscapes.

The effect of increased levels of capability in managing operational resilience on the mission assurance of high-value services is discussed. Part Two includes a detailed treatment of the model's Generic Goals and Practices, which are sourced from CMMI and tailored for institutionalizing operational resilience management processes. Part Two also describes various approaches for using CERT-RMM, as well as considerations when applying a plan-do-check-act model for process improvement.

Part Three, CERT-RMM Process Areas, is a detailed view of the 26 CERT-RMM process areas. They are organized alphabetically by process area acronym. Each process area contains descriptions of goals, practices, and examples.

How to Use This Document

Part One of this document provides a foundational understanding of CERT-RMM whether or not you have previous experience with process improvement models.

If you have process improvement experience, particularly using models in the CMMI family, you should start with Section 1.4 in the Introduction, which describes the relationship between CERT-RMM and CMMI models. Reviewing Part Three will provide you with a baseline understanding of the process areas covered in CERT-RMM and how they may be similar to or differ from those in CMMI. Next, you should examine Part Two to understand how Generic Goals and Practices are used in CERT-RMM. Pay particular attention to the example blocks in the Generic Goals and Practices; they provide an illustration of how the capability dimension can be implemented in the CERT-RMM model.

If you have no process improvement experience, you should begin with the Introduction in Part One and continue sequentially through the document. The chapters are arranged to build understanding before you reach Part Three, the process areas.

Additional Information and Reader Feedback

CERT-RMM continues to evolve as more organizations use it to improve their operational resilience management processes. You can always find up-to-date information on the CERT-RMM model, including new process areas as they are developed and added, at www.cert.org/resilience. There you can also learn how CERT-RMM is being used for critical infrastructure protection and how it forms the basis for exciting research in the area of resilience measurement and analysis.

Your suggestions on improving CERT-RMM are welcome. For information on how to provide feedback, see the CERT website at www.cert.org/resilience/request-comment. If you have comments or questions about CERT-RMM, send email to rmm-comments@cert.org.

Abstract

Organizations in every sector—industry, government, and academia—are facing increasingly complex operational environments and dynamic risk environments. These demands conspire to force organizations to rethink how they manage operational risk and the resilience of critical business processes and services.

The CERT® Resilience Management Model (CERT®-RMM) is an innovative and transformative way to approach the challenge of managing operational resilience in complex, risk-evolving environments. It is the result of years of research into the ways that organizations manage the security and survivability of the assets that ensure mission success. It incorporates concepts from an established process improvement community to allow organizations to holistically mature their security, business continuity, and IT operations management capabilities and improve predictability and success in sustaining operations whenever disruption occurs.

This report describes the model's key concepts, components, and process area relationships and provides guidance for applying the model to meet process improvement and other objectives. One process area is included in its entirety; the others are presented in outline form. All of the CERT-RMM process areas are available for download at www.cert.org/resilience.

Part One: About the CERT® Resilience Management Model

Organizations in every sector—industry, government, and academia—face increasingly complex business and operational environments. They are constantly bombarded with conditions and events that can introduce stress and uncertainty that may disrupt the effective operation of the organization.

Stress related to managing operational resilience—the ability of the organization to achieve its mission even under degraded circumstances—can come from many sources. For example,

- Technology advances are helping organizations to automate business processes and make them more effective at achieving their missions. But the cost to organizations is that the technology often introduces complexities, takes specialized support and resources, and creates an environment that is rife with vulnerabilities and risks.
- Organizations increasingly depend on partnerships to achieve their mission. External partners provide essential skills and functions, with the aim of increasing productivity and reducing costs. As a result, the organization must expose itself to new risk environments. By employing a chain of partners to execute a business process, the organization cedes control of mission assurance in exchange for cost savings.
- The increasing globalization of organizations and their supply chains poses a problem for management in that governance and oversight must cross organizational and geographical lines like never before. And it must be acknowledged that the emerging worldwide sociopolitical environment is forcing organizations to consider threats and risks that have previously not been on their radar screens. Recent well-publicized events have changed the view of what is feasible and have expanded the range of outcomes that an organization must attempt to prevent and from which it must be prepared to recover.

All of these new demands conspire to force organizations to rethink how they perform operational risk management and how they address the resilience of critical business services and processes. The traditional, and typically compartmentalized, disciplines of security, business continuity, and IT operations must be expanded to provide protection and continuity strategies for critical services and supporting assets that are commensurate with these new operating complexities.

In addition, organizations lack a reliable means to answer the question, How resilient am I? They also lack the ability to assess and measure their capability for managing operational resilience (Am I resilient enough?), as they have no credible yardstick against which to measure. Typically, capability is measured by the way that an organization has performed during an event, or it is described in vague terms that cannot be measured. For example, when organizations are asked to describe how well they are managing resilience, they typically characterize success in terms of what hasn't happened: "We haven't been attacked; therefore we must be doing everything right." Because there will always be new and emerging threats, knowing how well the organization performed today is necessary but not sufficient; it is more important to be able to predict how it will perform in the future when the risk environment changes.

CERT recognizes that organizations face challenges in managing operational resilience in complex environments. The solution to addressing these challenges must have several

dimensions. First and foremost, it must consider that the management activities for security, business continuity, and IT operations—typical operational risk management activities—are converging toward a continuum of practices that are focused on managing operational resilience. Second, the solution must address the issues of measurement and metrics, providing a reliable and objective means for assessing capability and a basis for improving processes. And finally, the solution must help organizations improve deficient processes—to reliably close gaps that ultimately translate into weaknesses that diminish operational resilience and impact an organization's ability to achieve its strategic objectives.

As a process improvement model, the CERT Resilience Management Model seeks to allow organizations to use a process definition as a benchmark for identifying the current level of organizational capability, setting an appropriate and attainable desired target for performance, measuring the gap between current performance and targeted performance, and developing action plans to close the gap. By using the model's process definition as a foundation, the organization can obtain an objective characterization of performance not only against a base set of functional practices but also against practices that indicate successively increasing levels of capability. *The CERT Resilience Management Model is the first known model in the security and continuity domain that includes a capability dimension. This provides an organization a means by which to measure its ability to control operational resilience and to consistently and predictably determine how it will perform under times of stress, disruption, and changing risk environments.*

1 Introduction

> *Operational resilience is the* ***emergent*** *property of an* ***organization*** *that can* ***continue to carry out its mission*** *after* ***disruption*** *that does not exceed its* ***operational*** *limit.* [1]

The CERT® Resilience Management Model (CERT-RMM) is the result of many years of research and development committed to helping organizations meet the challenge of managing operational risk and resilience in a complex world. It embodies the process management premise that "the quality of a system or product is highly influenced by the quality of the process used to develop and maintain it" by defining *quality* as the extent to which an organization controls its ability to operate in a mission-driven, complex risk environment [CMMI Product Team 2006].

CERT-RMM brings several innovative and advantageous concepts to the management of operational resilience.

- First, it seeks to holistically improve risk and resilience management through purposeful and practical convergence of the disciplines of security management, business continuity management, and aspects of IT operations management. (The convergence advantage.)
- Second, it elevates these disciplines to a process approach, which enables the application of process improvement innovations and provides a useful basis for metrics and measurement. It also provides a practical organizing and integrating framework for the vast array of practices in place in most organizations. (The process advantage.)
- Finally, it provides a foundation for process institutionalization and organizational process maturity—concepts that are important for sustaining any process but are absolutely critical for processes that operate in complex environments, typically during times of stress. (The maturity advantage.)

CERT-RMM v1.0 contains 26 process areas that cover four areas of operational resilience management: enterprise management, engineering, operations, and process management. The practices contained in these process areas are codified from a management perspective; that is, the practices focus on the activities that an organization performs to actively *direct, control, and manage* operational resilience in an environment of uncertainty, complexity, and risk. For example, the model does not prescribe specifically how an organization should secure information; instead, it focuses on the equally important processes of identifying critical information assets, making decisions about the levels needed to protect and sustain these assets, implementing strategies to achieve these levels, and maintaining these levels throughout the life cycle of the assets during stable times and, more importantly, during times of stress. In essence, the managerial focus supports the specific actions taken to secure information by making them more effective and more efficient.

[1] Adapted from a WordNet definition of resilience at http://wordnetweb.princeton.edu/perl/webwn?s=resilience.

1.1 The Influence of Process Improvement and Capability Maturity Models

Throughout its history, the Software Engineering Institute (SEI) has directed its research efforts toward helping organizations to develop and maintain quality products and services, primarily in the software and systems engineering and acquisition processes. Proven success in these disciplines has expanded opportunities to extend process improvement knowledge to other areas such as the quality of service delivery (as codified in the CMMI for Services (CMMI-SVC) model) and to cyber security and resilience management (CERT-RMM.)

The SEI's research in product and service quality reinforces three critical dimensions on which organizations typically focus: people, procedures and methods, and tools and equipment [CMMI Product Team 2006]. However, processes link these dimensions together and provide a conduit for achieving the organization's mission and goals across all organizational levels. Figure 1 illustrates these three critical dimensions.

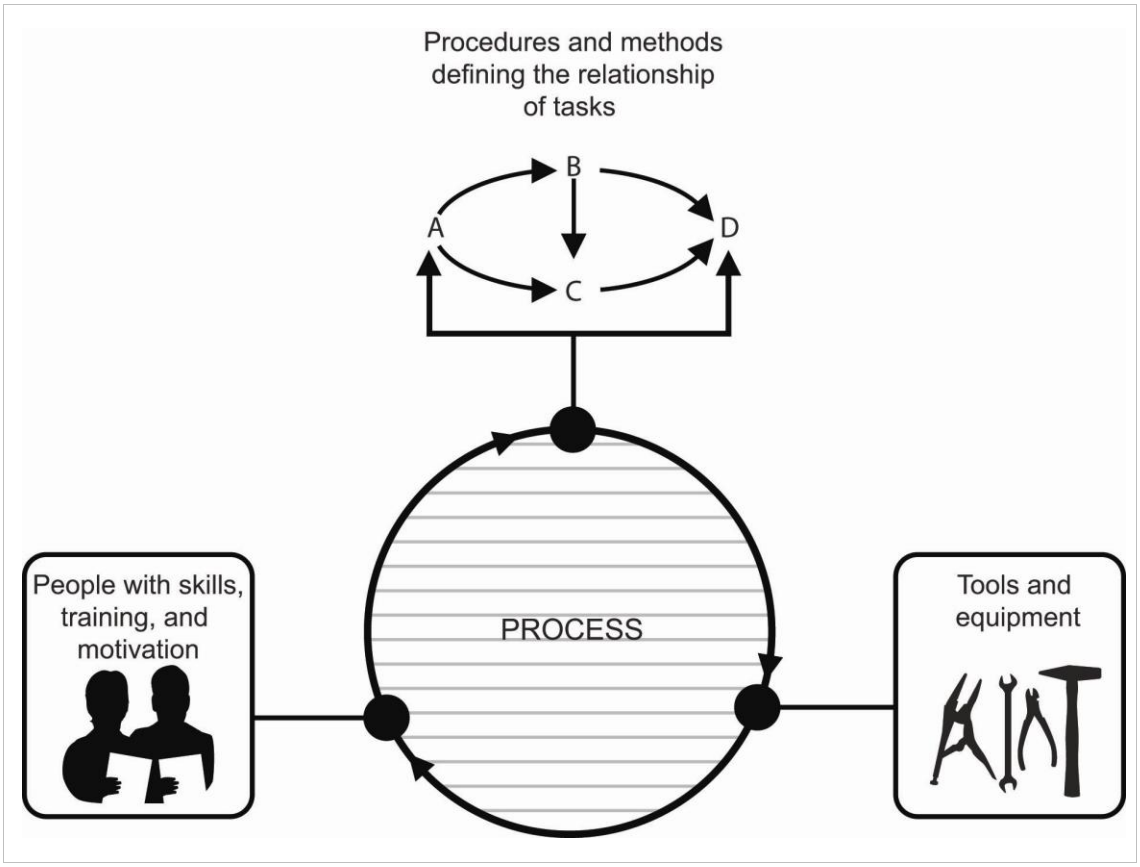


Figure 1: The Three Critical Dimensions

Traditionally, the disciplines concerned with managing operational risk have taken a technology-centric view of improvement. That is, of the three critical dimensions, organizations often look to technology—in the form of software-based tools and hardware—to fix security problems, to enable continuity, or even to improve IT operations and service delivery. Technology can be very effective in managing risk, but technology cannot always substitute for skilled people and resources, procedures and methods that define and connect tasks and activities, and processes to provide structure and stability toward the achievement of common objectives and goals. In our

experience, organizations often ask for the one or two technological advances that will keep their data secure or improve the way they handle incidents, while failing to recognize that the lack of defined processes and process management diminishes their overall capability for managing operational resilience. Most organizations are already technology-savvy when it comes to security and continuity, but the way they *manage* these disciplines is immature. In fact, incidents such as security breaches often can be traced back to poorly designed and managed processes at the enterprise and operational levels, not technology failures. Consider the following: your organization probably has numerous firewall devices deployed across its networks. But what kinds of traffic are these firewalls filtering? What rulesets are being used? Do these rulesets reflect management's resilience objectives and the needs for protecting and sustaining the assets with firewalls? Who sets and manages the rulesets? Under whose direction? All of these questions typify the need to augment technology with process so that the technology supports and enforces strategic objectives.

In addition to being technology-focused, many organizations are practice-focused. They look for a representative set of practices to solve their unique operational resilience management challenges and end up with a complex array of practices sourced from many different bodies of knowledge. The effectiveness of these practices is measured by whether they are used or "sanctioned" by an industry or satisfy a compliance requirement *instead of* how effective they are in helping the organization reduce exposure or improve predictability in managing impact. The practices are not the problem; organizations go wrong in assuming that practices *alone* will bring about a sustainable capability for managing resilience in a complex environment.

Further damage is done by practice-based assessments or evaluations. Simply verifying the existence of a practice sourced from a body of knowledge does not provide for an adequate characterization of the organization's ability to *sustain* that practice over the long term, particularly when the risk environment changes or when disruption occurs. This can only be done by examining the degree to which the organization embeds the practice in its culture, is able and committed to performing the practice, can control the practice and ensure the practice is effective through measurement and analysis, and can prove the practice is performed according to established procedures and processes. In short, practices are made better by the degree to which they have been institutionalized through *processes*.

1.2 The Evolution of CERT-RMM

The CERT Resilience Management Model is the result of an evolutionary development path that incorporates concepts from other CERT tools, techniques, methods, and activities.

In 1999, CERT officially released the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method for information security risk management. OCTAVE provided a new way to look at information security risk from an operational perspective and asserted that business people are in the best position to identify and analyze security risk. This effectively repositioned IT's role in security risk assessment and placed the responsibility closer to the operations activity in the organization [Alberts 1999].

In October 2003, a group of 20 information technology (IT) and security professionals from financial, IT, and security services, defense organizations, and the SEI met at the SEI to begin to build an executive-level community of practice for IT operations and security. The desired

outcome for this Best in Class Security and Operations Roundtable (BIC-SORT) was to better capture and articulate the relevant bodies of knowledge that enable and accelerate IT operational and security process improvement. The bodies of knowledge identified included IT and information security governance, audit, risk management, IT operations, security, project management, and process management (including benchmarking), as depicted in Figure 2.

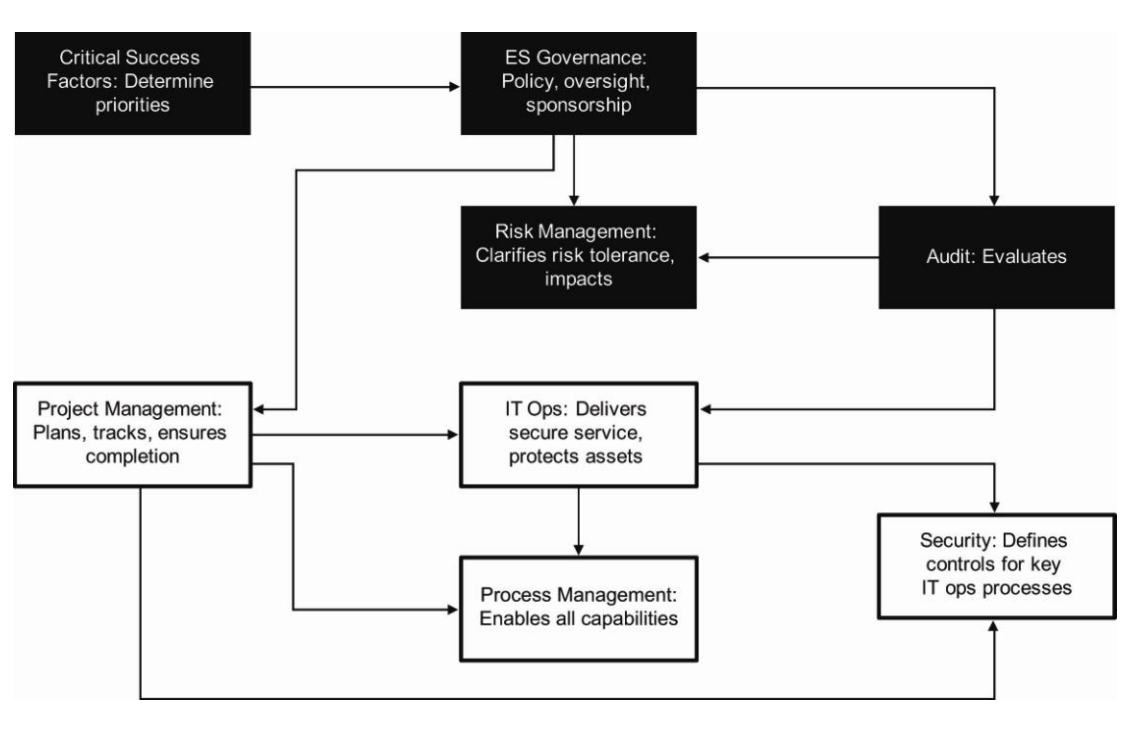


Figure 2: Bodies of Knowledge Related to Security Process Improvement

In Figure 2, the upper four capabilities (white text) include processes that provide oversight and top-level management. Enterprise security governance and audit serve as enablers and accelerators. Risk management informs decisions and choices. Critical success factors serve as the explicit link to business drivers to ensure that value is being delivered. The lower four capabilities (black text) include processes that provide detailed management and execution in accordance with the policies, procedures, and guidelines established by senior management. We observed that these capabilities were all connected in high-performing IT operations and security organizations.

Workshop topics and results included defining what it means to be best in class, areas of pain and promise (potential solutions), how to use improvement frameworks and models in this domain, the applicability of Six Sigma, and emerging frameworks for enterprise security management (precursors of CERT-RMM) [Allen 2004].

In December 2004, CERT released a technical note entitled *Managing for Enterprise Security* that described security as a process reliant on many organizational capabilities. In essence, the security challenge was characterized as a business problem owned by everyone in the organization, not just IT [Caralli 2004]. This technical note also introduced operational resilience as the objective of security activities and began to describe the convergence between security management, business

continuity management, and IT operations management as essential for managing operational risk.

In March 2005, CERT hosted a meeting with representatives of the Financial Services Technology Consortium (FSTC).[2] At the time of this 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 resilience capability. Although our approaches to operational resilience had different starting points (security versus business continuity), our efforts were clearly focused on solving the same problem: How can an organization predictably and systematically control operational resilience through activities such as security and business continuity?

In April 2006, as a result of work with FSTC, CERT published an initial framework for managing operational resilience in the technical report *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* [Caralli 2006]. This technical report formed the basis for the first expression of the model.

In March 2008, a preview version of a process improvement model for managing operational resilience was released by CERT under the title The CERT Resiliency Engineering Framework, v0.95R [REF Team 2008a]. This model included an articulation of 21 "capability areas" that described high-level processes and practices for managing operational resilience and, more significantly, provided an initial set of elaborated generic goals and practices that defined capability levels for each capability area.

In early 2009, the name of the model was changed to the CERT Resilience Management Model to reflect the managerial nature of the processes and to properly position the "engineering" aspects of the model. Common CMMI-related taxonomy was applied (including the use of the term "process areas"), and generic goals and practices were expanded with more specific elaborations in each process area. CERT began releasing CERT-RMM process areas individually in 2009, leading up to the "official" release of v1.0 of the model in this technical report. The model continues to be available by process area at www.cert.org/resilience.

1.3 CERT-RMM

CERT-RMM draws upon and is influenced by many bodies of knowledge and models. Figure 3 illustrates these relationships. (See Tables 1 and 2 for details about the connections between CERT-RMM and CMMI models.)

[2] FSTC has since been incorporated into the Financial Services Roundtable (www.fsround.org).

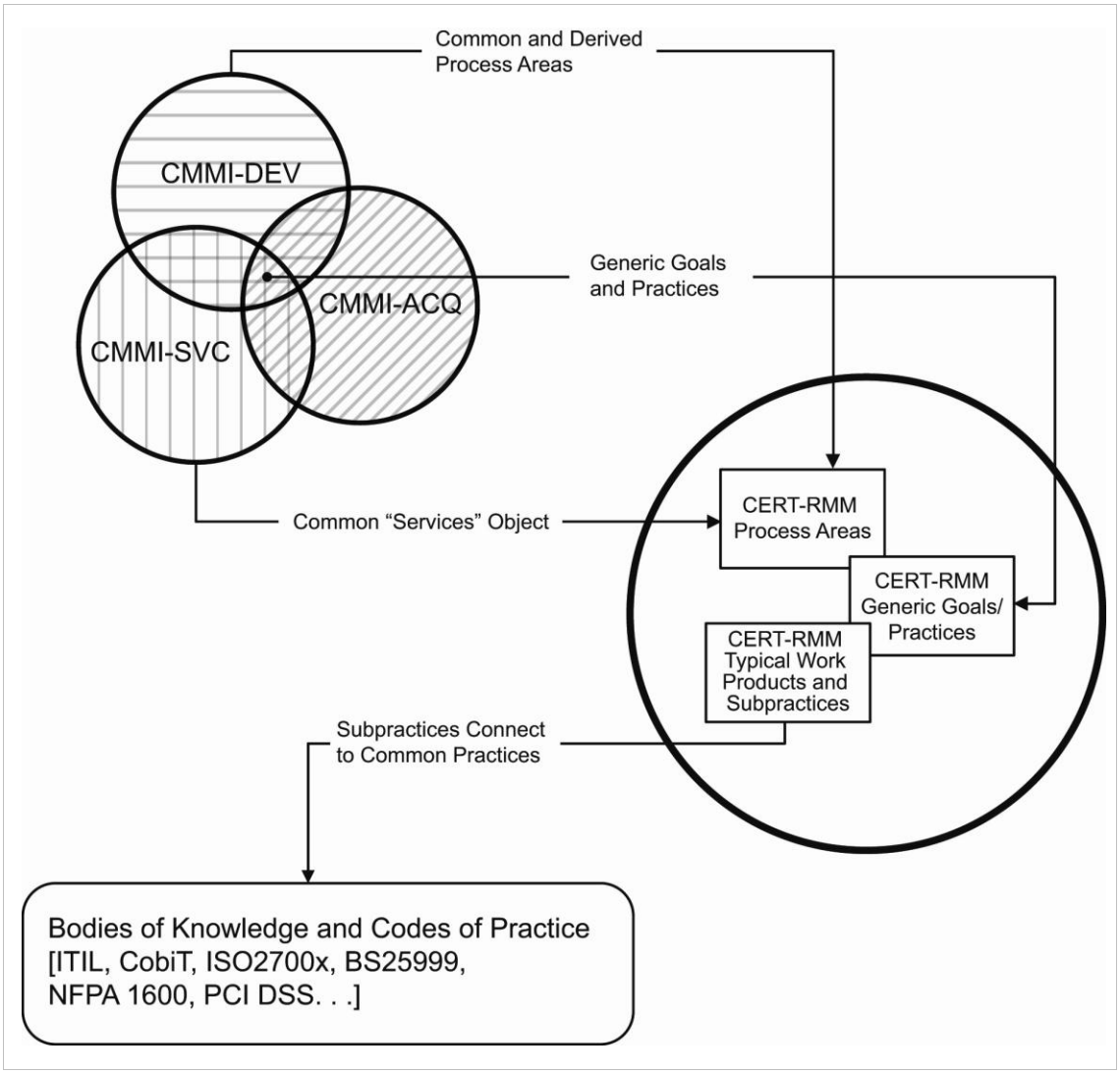


Figure 3: CERT-RMM Influences

At the descriptive level of the model, the process areas in CERT-RMM have either been developed specifically for the model or sourced from existing CMMI models and modified to be used in the context of operational resilience management. CERT-RMM also draws upon concepts and codes of practice from other security, business continuity, and IT operations models, particularly at the typical work products and subpractices level. This allows users of these codes of practice to incorporate model-based process improvement without significantly altering their installed base of practices. The *CERT-RMM Code of Practices Crosswalk v0.95R* [REF Team 2008b] details the relationships between common codes of practice and the specific practices in the CERT-RMM process areas. The Crosswalk is periodically updated to incorporate new and updated codes of practice as necessary. The Crosswalk can be found at www.cert.org/resilience.

Familiarity with common codes of practice or CMMI models is not required to comprehend or use CERT-RMM. However, familiarity with these practices and models will aid in understanding and adoption.

As a descriptive model, CERT-RMM focuses at the process description level but doesn't necessarily address how an organization would achieve the intent and purpose of the description through deployed practices. However, the subpractices contained in each CERT-RMM process area describe actions that an organization might take to implement a process, and these subpractices can be directly linked to one or more tactical practices used by the organization. Thus, the range of material in each CERT-RMM process area spans from highly descriptive processes to more prescriptive subpractices.

In terms of scope, CERT-RMM covers the activities required to establish, deliver, and manage operational resilience activities in order to ensure the resilience of services. A resilient service is one that can meet its mission whenever necessary, even under degraded circumstances. Services are broadly defined in CERT-RMM. At a simple level, a service is a helpful activity that brings about some intended result. People and technology can perform services; for example, people can deliver mail, and so can an email application. A service can also produce a tangible product.

From an organizational perspective, services can provide internal benefits (such as paying employees) or have an external focus (such as delivering newspapers). Any service in the organization that is of value to meeting the organization's mission should be made resilient.

Services rely on assets to achieve their missions. In CERT-RMM, assets are limited to people, information, technology, and facilities. A service that produces a product may also rely on raw materials, but these assets are outside of the immediate scope of CERT-RMM. However, the use of CERT-RMM in a production environment is not precluded, since people, information, technology, and facilities are a critical part of delivering a product, and their operational resilience can be managed through the practices in CERT-RMM.

CERT-RMM does not cover the activities required to establish, deliver, and manage services. In other words, CERT-RMM does not address the development of a service from requirements or the establishment of a service system. These activities are covered in the CMMI-SVC model [CMMI 2009]. However, to the extent that the management of the service requires a strong resilience consideration, CERT-RMM can be used with CMMI-SVC to extend the definition of high-quality service delivery to include resilience as an attribute of quality.

CERT-RMM contains practices that cover enterprise management, resilience engineering, operations management, process management, and other supporting processes for ensuring active management of operational resilience. The "enterprise" orientation of CERT-RMM does not mean that it is an enterprise-focused model or that it must be adopted at an enterprise level; on the contrary, CERT-RMM is focused on the operations level of the organization, where services are typically executed. Enterprise aspects of CERT-RMM describe how horizontal functions of the organization, such as managing people, training, financial resource management, and risk management, affect operations. For example, if an organization is generally poor at risk management, the effects of this typically manifest at an operational level in poor risk identification, prioritization, and mitigation, misalignment with risk appetite and tolerances, and diminished service resilience.

CERT-RMM was developed to be scalable across various industries, regardless of their size. Every organization has an operational component and executes services that require a degree of operational resilience commensurate with achieving the mission. Although CERT-RMM was

constructed in the financial services industry, it is already being piloted and used in other industrial sectors and government organizations, both large and small.

Finally, understanding the process improvement focus of CERT-RMM can be tricky. An example from software engineering is a useful place to start. In the CMMI for Development model (CMMI-DEV), the focus of improvement is software engineering activities performed by a "project" [CMMI Product Team 2006]. In CERT-RMM, the focus of improvement is operational resilience management activities *to achieve service resilience* as performed by an "organizational unit." This concept can become quite recursive (but no less effective) if the "organizational unit" happens to be a unit of the organization that has primary responsibility for operational resilience management "services," such as the information security department or a business continuity team. In this context, the operational resilience management activities are also the services of the organizational unit.

1.4 CERT-RMM and CMMI Models

CMMI version 1.2 includes three integrated models: CMMI for Development (CMMI-DEV), CMMI for Acquisition (CMMI-ACQ), and the newly released CMMI-SVC. *The CMMI Framework* provides a common structure for CMMI models, training, and appraisal components. CMMI for Development and CMMI for Acquisition are early life-cycle models in that they address software and systems processes through the implementation phase but do not specifically address these assets in operation. The CMMI for Services model addresses not only the development of services and a service management system but also the operational aspects of service delivery.

CERT-RMM is primarily an operations-focused model, but it reaches back into the development phase of the life cycle for assets such as software and systems to ensure consideration of early life-cycle quality requirements for protecting and sustaining these assets once they become operational. Like CMMI for Services, CERT-RMM also explicitly addresses developmental aspects of services and assets by promoting a requirements-driven, engineering-based approach to developing and implementing resilience strategies that become part of the "DNA" of these assets in an operational environment.

Because of the broad nature of CERT-RMM, emphasis on using CMMI model structural elements was prioritized over explicit consideration of integration with existing CMMI models. That is, while CERT-RMM could be seen as defining an "operations" constellation in CMMI, this was not an early objective of CERT-RMM research and development. Instead, the architects and developers of CERT-RMM focused on the core processes for managing operational resilience, integrating CMMI model elements to the extent possible. Thus, because the model structures are similar, CMMI users will be able to easily navigate CERT-RMM.

Table 1 provides a summary of the process area connections between CERT-RMM and the CMMI models. Table 2 summarizes other CMMI model and CERT-RMM similarities. Future versions of CERT-RMM will attempt to smooth out significant differences in the models and incorporate more CMMI elements where necessary.

Table 1: Process Areas in CERT-RMM and CMMI Models

CMMI Models Process Areas	Equivalent CERT-RMM Process Areas
CAM – Capacity and Availability Management *(CMMI-SVC only)*	**TM – Technology Management** CERT-RMM addresses capacity management from the perspective of technology assets. It does not address the capacity of services. Availability management is a central theme of CERT-RMM, significantly expanded from CMMI-SVC. Service availability is addressed in CERT-RMM by managing the availability requirement for people, information, technology, and facilities. Thus, the process areas that drive availability management include • **RRD – Resilience Requirements Development** (where availability requirements are established) • **RRM – Resilience Requirements Management** (where the life cycle of availability requirements is managed) • **EC – Environmental Control** (where the availability requirements for facilities are implemented and managed) • **KIM – Knowledge and Information Management** (where the availability requirements for information are implemented and managed) • **PM – People Management** (where the availability requirements for people are implemented and managed) • **TM – Technology Management** (where the availability requirements for software, systems, and other technology assets are implemented and managed)
IRP – Incident Resolution and Prevention *(CMMI-SVC only)*	**IMC – Incident Management and Control** In CERT-RMM, IMC expands IRP to address a broader incident management system and incident life cycle at the asset level. Workarounds in IRP are expanded in CERT-RMM to address incident response practices.
MA – Measurement and Analysis	**MA – Measurement and Analysis** is carried over intact from CMMI. In CERT-RMM, MA is directly connected to MON – Monitoring, which explicitly addresses data collection that can be used for MA activities.
OPD – Organizational Process Definition	**OPD – Organizational Process Definition** is carried over from CMMI, but development life-cycle-related activities and examples are deemphasized or eliminated.
OPF – Organizational Process Focus	**OPF – Organizational Process Focus** is carried over intact from CMMI.
OT – Organizational Training	**OTA – Organizational Training and Awareness** OT is expanded to include awareness activities in OTA.
REQM – Requirements Management	**RRM – Resilience Requirements Management** Basic elements of REQM are included in RRM, but the focus is on managing the resilience requirements for assets and services, regardless of where they are in their development cycle.
RD – Requirements Development	**RRD – Resilience Requirements Development** Basic elements of RD are included in RRM, but practices differ substantially.

CMMI Models Process Areas	Equivalent CERT-RMM Process Areas
RSKM – Risk Management	**RISK – Risk Management** Basic elements of RSKM are reflected in RRM, but the focus is on operational risk management activities and the enterprise risk management capabilities of the organization.
SAM – Supplier Agreement Management	**EXD – External Dependencies Management** In CERT-RMM, SAM is expanded to address all external dependencies, not only suppliers. EXD practices differ substantially.
SCON – Service Continuity *(CMMI-SVC only)*	**SC – Service Continuity** In CERT-RMM, SC is positioned as an operational risk management activity that addresses what is required to sustain assets and services balanced with preventive controls and strategies (as defined in CTRL – Controls Management).
TS – Technical Solution	**RTSE – Resilient Technical Solution Engineering** RTSE uses TS as the basis for conveying the consideration of resilience attributes as part of the technical solution.

Table 2: Other Connections Between CERT-RMM and the CMMI Models

Element	Connection
Generic goals and practices	The generic goals and practices have been adapted mostly intact from CMMI. Slight modifications have been made as follows: • The numbering scheme used in CERT-RMM uses GG.GP notation. For example, GG1.GP2 is generic goal 1, generic practice 2. • Generic practice 2.1 in CMMI focuses on policy, but in CERT-RMM it is expanded to address governance, with policy as an element. • Generic practice 2.6 in CMMI is ~~"M~~anage Configurations," but in CERT-RMM it is clarified to explicitly focus on ~~"w~~ork product" configurations to avoid confusion with traditional configuration management activities as defined in IT operations.
Continuous representation	CERT-RMM adopts the continuous representation concept from CMMI intact.
Capability levels	CERT-RMM defines four capability levels up to Capability Level 3 – Defined. Definitions of capability levels in CMMI are carried over for CERT-RMM.
Appraisal process	The CERT-RMM capability appraisal process uses many of the elements of the SCAMPI process. The ~~"p~~roject" concept in CMMI is implemented in CERT-RMM as an ~~"o~~rganizational unit." CERT-RMM capability appraisals have constructs inherited from SCAMPI. See Section 6.4.1 for the use of SCAMPI in CERT-RMM capability appraisals.

1.5 Why CERT-RMM Is Not a Capability *Maturity* Model

The development of maturity models in the security, continuity, IT operations, and resilience space is increasing dramatically. This is not surprising, since models like CMMI have proven

their ability to transform the way that organizations and industries work. Unfortunately, not all maturity models contain the rigor of models like CMMI, nor do they accurately deploy many of the maturity model constructs used successfully by CMMI. It is important to have some basic knowledge about the construction of maturity models in order to understand what differentiates CERT-RMM and why the differences ultimately matter.

In its simplest form, a maturity model is an organized way to convey a path of experience, wisdom, perfection, or acculturation. The subject of a maturity model can be an object or things, ways of doing something, characteristics of something, practices, or processes. For example, a simple maturity model could define a path of successively improved tools for doing math: using fingers, using an abacus, using an adding machine, using a slide rule, using a computer, or using a hand-held calculator. Thus, using a hand-held calculator may be viewed as a more mature tool than a slide rule.

A capability maturity model (in the likeness of CMMI) is a much more complex instrument, with several distinguishing features. One of these features is that the maturity dimension in the model is a characterization of the maturity of *processes*. Thus, what is conveyed in a capability maturity model is the degree to which processes are institutionalized and the organization demonstrates process maturity.

As you will learn in Chapter 5, these concepts correlate to the description of the "levels" in CMMI. For example, at the "defined" level, the characteristics of a defined process (governed, staffed with trained personnel, measured, etc.) are applied to a software or systems engineering process. Likewise for the "managed" level, where the characteristics of a managed process are applied to software or systems engineering processes. Unfortunately, many so-called maturity models that claim to be based on CMMI attempt to use CMMI maturity level descriptions, yet do not have a *process* orientation.

Another feature of CMMI—as implied by its name—is that there are really two maturity dimensions in the model. The *capability dimension* describes the degree to which a process has been institutionalized. Institutionalized processes are more likely to be retained during times of stress. They apply to an individual process area, such as incident management and control. On the other hand, the *maturity dimension* is described in maturity levels, which define levels of organizational maturity that are achieved through raising the capability of a *set of process areas* in a manner prescribed by the model.

From the start, the focus in developing CERT-RMM was to describe operational resilience management from a process perspective, which would allow for the application of process improvement tools and techniques and provide a foundational platform for better and more sophisticated measurement methodologies and techniques. The ultimate goal in CERT-RMM is to ensure that operational resilience processes produce intended results (such as improved ability to manage incidents or an accurate asset inventory), and as the processes are improved, so are the results and the benefits to the organization. Because CERT-RMM is a process model at its core, it was perfectly suited for the application of CMMI's capability dimension. Thus, the model contained in this book describes a *capability model*—grounded in process and providing a path for improving capability. CERT-RMM, however, is not a capability *maturity* model, *yet*. Describing organizational maturity for managing operational resilience by defining a prescriptive path through the model (i.e., by providing an order by which process areas should be addressed)

requires additional study and research, and all indications from early model use, benchmarking, and piloting is that a capability maturity model for operational resilience management is achievable in the future.

2 Understanding Key Concepts in CERT-RMM

Several key terms and concepts are noteworthy, as they form the foundation for CERT-RMM. Although all are defined in the glossary, they each employ words with multiple possible meanings and interpretations to those with different backgrounds. So they merit some additional discussion to ensure that CERT-RMM content that uses and builds on these concepts is correctly interpreted.

2.1 Foundational Concepts

2.1.1 Disruption and Stress

The objective of many capability and maturity models is to improve the processes associated with building, developing, or acquiring the target object of the model, such as the development and acquisition of a particular product or service or the enhancement of workforce competencies and skills. CERT-RMM differs in that its focus is on improving how organizations behave and respond in advance of and during times of stress and disruption. So, for example, the objective of CMMI-SVC is to deliver high-quality services. The objective of CERT-RMM is to ensure that high-quality services are resilient in the face of stress and disruption.[3]

Organizations are constantly bombarded with events and conditions that can cause stress and may disrupt their effective operation. Controlling organization behavior and response during times of disruption and stress is a primary focus of operational resilience management—the ability to adapt to operational risks, including realized risks.

Stress related to managing operational risk, and thus operational resilience, can come from many sources, including

- pervasive use of technology
- operational complexity
- increased reliance on intangible assets, such as digital information and software
- global economy and economic pressures
- open borders
- geopolitical and cultural shifts
- regulatory and legal constraints
- a view of security as an IT problem, not an organization-wide concern

The explosion of computing power and cheap storage means that *technology* is in everyone's hands. Technology is a critical enabler of most of the organization's important products, services, and processes. It is constantly changing and provides increasing opportunities for operational risk, organizational stress (including stress to an organization's supply chain), and disruption.

[3] CMMI-SVC achieves its objective by focusing on the improvement of the service management and delivery process, with services as the object of improvement. CERT-RMM achieves its objectives by focusing on the improvement of the operational resilience management process, with services as the beneficiary of improvement.

More and changing technology often means more *complexity*. While the automation of manual and mechanical processes through the application of technology makes these processes more productive, it also makes them more complex. Implementation of new technologies can introduce new risks that are not identified until they are realized. And technological advances, while providing demonstrable opportunities for improvements in effectiveness and efficiency, often increase the likelihood that something will go wrong.

The number and extent of *intangible and virtual assets*, such as digital information, software, and supply chain products and services, are rapidly increasing [Caralli 2006, pg. 40]. Intangibility may increase the likelihood and impact of potential risks. Intangible assets are more challenging to identify, locate, and therefore protect, and protection levels are difficult to sustain without concerted effort. This quality of digital assets forces organizations to pay more attention to the convergence of cyber and physical security issues because the controls to protect and sustain these must work together.

Trading in a *global economy* provides less insulation from global risks and, correspondingly, less control. Economic disruptions and downturns often result in increased cyber attacks and increased risk to global supply chain products, services, and partners. People often change their behavior during uncertain economic times, so the potential for insider threats and attacks may also increase.

Participation in the global economy brings a requirement for more *open borders* to compete and thrive. Open borders can introduce additional stress when organizational core competencies are outsourced to realize cost savings. Outsourcing can often cause such core competencies to diminish or disappear altogether, which makes it difficult to competently manage outsourced partners. Open borders extend the risk environment to arenas, partners, and countries that are often unknown and untested. In addition, transferring functions to outsourced partners often means the transfer of risk management, even though the primary organization continues to be the owner and responsible party for ensuring that the risks associated with outsourced products and services are sufficiently mitigated.

Having supply chain partners in other countries can introduce additional stress and potential disruption when navigating *cultural* norms and conducting business in non-native languages. It also can cause an organization to be affected by *political instability* such as governments at risk (and thus unable to fulfill their agreements) and economically linked worker protests. Organizations need to be cognizant of any region that may harbor terrorists with antinational sentiments. In addition, too much presence in a country can result in outsourcing backlash and financial services backlash directed toward the primary organization attempting to conduct business in the region.

All business leaders are well aware of the increasing requirements and constraints introduced by the growing number of *laws and regulations* with which they are expected to comply. Assessing for and ensuring compliance can be costly, not only in labor resources but also in opportunity costs. Many organizations, in an attempt to be fully compliant, adopt a prescriptive, checklist-like approach to assessing compliance and thus a prescriptive view of the risks that may result from non-compliance. This prohibits them from fully articulating their risk exposure and likely over-investing in controls for compliance that may not be necessary.

Historically and often still today, *security is viewed as a technology problem* and thus relegated to the IT department. As a result, the budgets for managing operational risk for information technologies often reside with IT, not in the business units that are most likely to be impacted when operational risks are realized. Most organizations address risk management, security (both physical and cyber), business continuity, disaster recovery, and IT operations as siloed, compartmentalized functions with little to no integration and communication even though they share many of the same issues, solutions, and core competencies. When an incident or disruption occurs, the response is generally localized and discrete, not orchestrated across all affected lines of business and organizational units. This condition calls for harmonization and convergence, which is addressed next.

2.1.2 Convergence

Convergence is a fundamental concept for managing operational resilience. For CERT-RMM purposes, it is defined as the harmonization of operational risk management activities that have similar objectives and outcomes.[4] These activities include

- security planning and management
- business continuity and disaster recovery management
- IT operations and service delivery management

Other support activities are typically included, such as financial management, communications, human resource management, and organizational training and awareness. This concept is depicted in Figure 4.

Figure 4: Convergence of Operational Risk Management Activities

Many organizations are now beginning to realize that security, business continuity, and IT operations management are complementary and collaborative functions that have the same goal: to improve and sustain operational resilience. They share this goal because each function is

[4] These activities are bound by their operational risk focus. However, collectively they do not represent the full range of activities that define operational risk management.

focused on managing operational risk. This convergent view is often substantiated by popular codes of practice in each domain. For example, security practices now explicitly reference and include business continuity and IT operations management practices as an acknowledgement that security practices alone do not address both the conditions and consequences of risk. Thus the degree or level to which convergence has been achieved directly affects the level of operational resilience for the organization. Correspondingly, the level of operational resilience affects the ability of the organization to meet its mission.

The business case for convergence ultimately comes down to economics. When organizational functions and activities share many of the same objectives, issues, solutions, and core competencies, it makes good business sense to tackle these using a common, collaborative approach. Security planning and management, business continuity and disaster recovery management, and IT operations and service delivery management are bound by the same operational risk drivers. A convergent approach allows for better alignment between risk-based activities and organizational risk tolerances and appetite. In other words, such activities are likely to have risks in common with similar thresholds that can be managed and mitigated using similar, if not identical, approaches.

Redundant activities can be eliminated along with their associated costs. Staff resources can be more effectively deployed and optimized. Convergence enforces a focus on organizational and service missions. It facilitates a process that is owned by line of business and organizational unit managers and consistently implemented across the organization. A common, collaborative approach greatly influences how operational risk and operational resilience management work is planned, executed, and managed to the end objective of greater effectiveness, efficiency, and reduced risk exposure.

If this is such an obvious win, what gets in the way? These activities and functions (and the people who perform them) have a long history of working independently. Organizational structures and traditional funding models tend to solidify this separation. Numerous codes of practice for each discipline exist, reinforcing their separateness. Compliance drives their use, rather than performance. Misuse sustains an entrenched and isolated view of who should be doing what. Risk drivers that apply to all of these activities are unclear, poorly defined, and not communicated. The same can be said for enterprise and strategic objectives and critical success factors that are intended to drive all of these activities. Governance and visible sponsorship for converged activities is rarely present; this is also the case for developing a process orientation and process definition for converged activities.

2.1.3 Managing Operational Resilience

The demands and stress factors described above conspire to force organizations to rethink how they perform some aspects of operational risk management and how they address the resilience of high-value business processes and services. Security, business continuity, and IT operations comprise a large segment of operational risk management activities for almost all organizations.

Operational risk is defined as the potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events. To more effectively manage and mitigate operational risk requires that an organization focus its attention on operational resilience.

Operational resilience addresses the organization's ability to adapt to risk that affects its core operational capacities. It is an emergent property of effective and efficient operational risk management [Caralli 2006].

Operational resilience management defines the processes and related practices that an organization uses to design, develop, implement, and control the strategies to protect and sustain (i.e., make operationally resilient) high-value (organizationally critical) services, related business processes, and associated assets such as people, information, technology, and assets. Operational resilience management

- includes both developmental (build, acquire) and operational (manage) aspects
- actualizes the concept of convergence
- characterizes an active and directly controlled activity, rather than a passive activity

Simply put, comprehensive management of operational resilience includes four objectives:

- Prevent the realization of operational risk to a high-value service (instantiated by a protect strategy).
- Sustain a high-value service if risk is realized (instantiated by a sustain strategy).
- Effectively address consequences to the organization if risk is realized, and return the organization to a "normal" operating state.
- Optimize the achievement of these objectives to maximize effectiveness at the lowest cost.

Requirements form the basis for managing operational resilience. Protect and sustain strategies for an organizational service and associated assets are based on resilience requirements that reflect how the service and assets are used to support the organization's strategic objectives. When the organization fails to meet these requirements (either because of poor practices or as a result of an incident, disaster, or other disruptive event), the operational resilience of the service and assets is diminished, the service mission is at risk, and thus one or more of the organization's strategic objectives is not met. Thus, operational resilience depends on establishing requirements in order to build resilience into assets and services and to keep these assets and services productive in the accomplishment of strategic objectives.

Through extensive review of existing codes of practice in the areas of security, business continuity, and IT operations management, as well as from experience with helping organizations to adopt a convergent view, CERT developers have codified in CERT-RMM a process definition for resilience management processes. The process definition embodies a requirements-driven foundation and describes the range of processes that characterize the organizational capabilities necessary to actively direct, control, and manage operational resilience.

2.2 Elements of Operational Resilience Management

CERT-RMM defines several foundational concepts that provide useful levels of abstraction applied throughout the model. These concepts include

- services
- business processes
- assets

- resilience requirements
- strategies for protecting and sustaining assets and services
- life-cycle coverage

These concepts are key to understanding CERT-RMM's process-based approach to managing operational resilience. All are described in the sections that follow. Figure 5 depicts the relationship between services, business processes, and CERT-RMM assets.

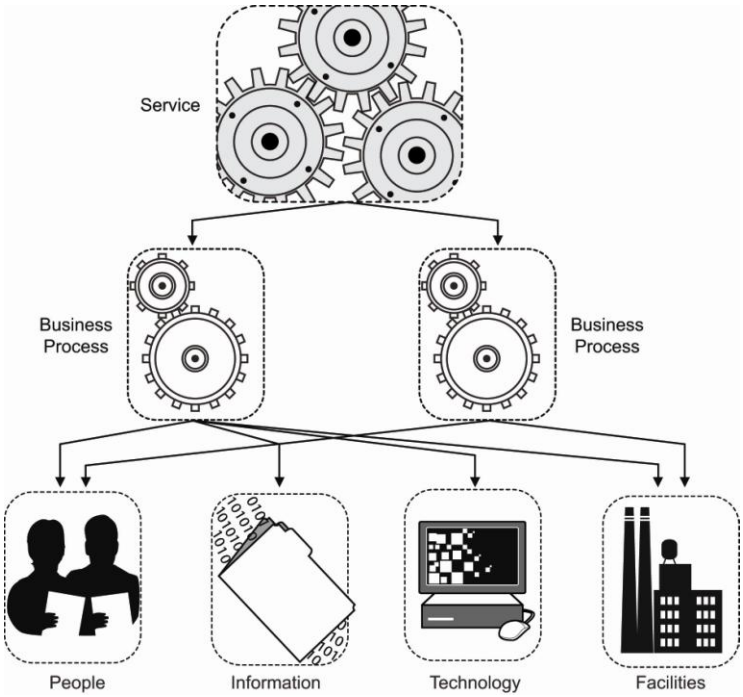


Figure 5: Relationships Among Services, Business Processes, and Assets

2.2.1 Services

A service is the limited number of activities that the organization carries out in the performance of a duty or in the production of a product.[5] In the gas utilities industry, services include gas production, gas distribution, and gas transmission. In the financial services sector, services include retail/consumer banking, commercial banking, and loan processing. Services can be externally focused and customer-facing, such as the production of shrink-wrapped software or providing web services for conducting market surveys. Services can be internally focused, such as human resources transactions (hiring, performance reviews) and monthly financial reporting. Services typically align with a particular line of business or organizational unit but can cross units and organizational boundaries (such as in the case of a global supply chain to produce an automobile). While the focus of CERT-RMM is on processes for managing operational resilience,

[5] In the CMMI for Services model, a service is defined as a product that is intangible and non-storable [CMMI Product Team 2009]. CMMI for Services focuses on the high-quality delivery of services. CERT-RMM extends this concept by focusing on resilience as an attribute of high-quality service delivery, which ultimately impacts organizational health and resilience. In CERT-RMM, services are used as an organizing principle; the resilience of these services is the focus of improving operational resilience management processes.

resilience of services is key for mission assurance. Thus one of the foundational concepts in CERT-RMM is that improving operational resilience management processes has a significant, positive effect on service resilience. Figure 6 depicts the relationship between services and operational resilience management processes.

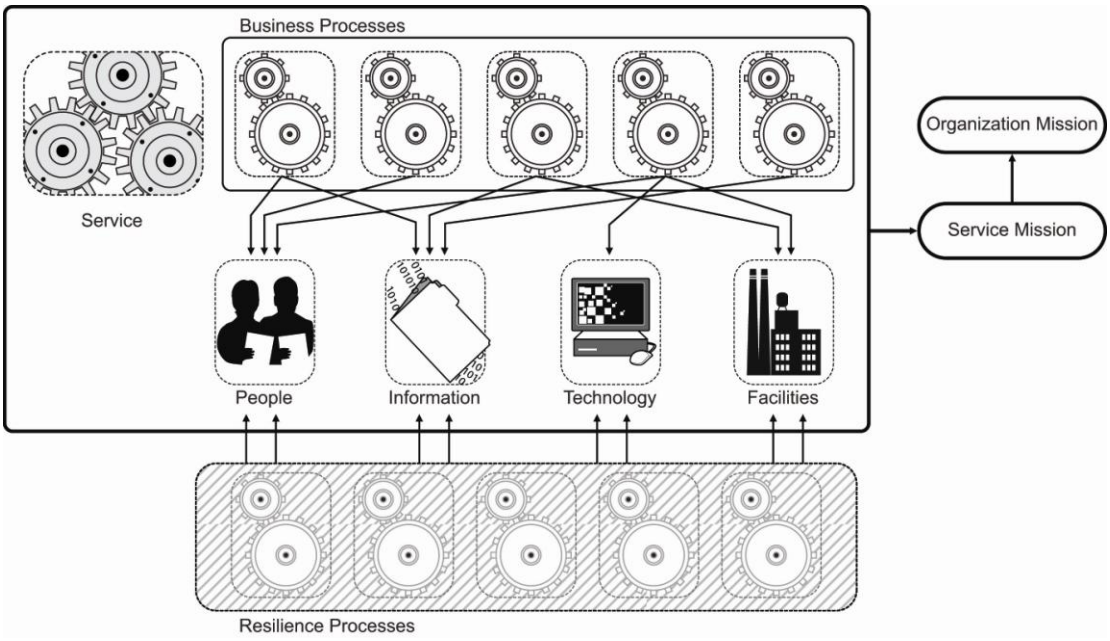


Figure 6: Relationship Between Services and Operational Resilience Management Processes

So what makes a service resilient? CERT-RMM identifies the following activities as contributing to service resilience:

- identification and mitigation of risks to the service and its supporting assets (see "Assets" in Section 2.2.3)
- implementation of service continuity processes and plans
- management and deployment of people, including external partners
- management of IT operations
- identification and deployment of effective controls for information and technology assets
- management of the operational environment where services are performed

A key aspect of services is the concept of *high-value* services, those that are critical to the success of the organization's mission. The high-value services of the organization are the focus of the organization's operational resilience management activities. These services directly support the achievement of strategic objectives and therefore must be protected and sustained to the extent necessary to minimize disruption. Failure to keep these services viable and productive may result in significant inability to meet strategic objectives and, in some cases, the organization's mission. To appropriately scope the organization's operational resilience management processes and corresponding operational resilience management activities, the high-value services of the organization must be identified, prioritized, and communicated as a common target for success. High-value services serve as the focus of attention throughout CERT-RMM as the means by which to establish priorities for managing risk and improving processes, given that it is not

possible (nor does it make good business sense) to mitigate all risks and improve all processes. High-value services are fueled by organizational assets such as people, information, technology, and facilities.

2.2.2 Business Processes

A business process is a series of discrete activities or tasks that contribute to the fulfillment of a service mission. Think of a business process as the next level of decomposition for a service, and a service as the aggregation of all of the business processes necessary for service success. A single business process may support multiple services. As with services, business processes can traverse the organization and cross organizational lines. In addition, business processes are often performed outside of the boundaries of the organization. Each business process mission must enable the service mission it supports. In the CERT-RMM, any discussion of services can be understood to be referring to all their component business processes as well.

2.2.3 Assets

An asset is something of value to the organization. Services and business processes are "fueled" by assets—the raw materials that services need to operate.[6] A service cannot accomplish its mission unless there are

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

Success at achieving the organization's mission relies on critical dependencies between organizational goals and objectives, services, and associated high-value assets. Operational resilience starts at the asset level. To ensure operational resilience at the service level, related assets must be protected from threats and risks that could disable them. Assets must also be sustainable (able to be recovered and restored to a defined operating condition or state) during times of disruption and stress. The optimal mix of protect and sustain strategies depends on performing tradeoff analysis that considers the value of the asset and the cost of deploying and maintaining the strategy.

As shown in Figure 7, failure of one or more assets (due to disruptive events, realized risk, or other issues) has a cascading impact on the mission of related business processes, services, and the organization as a whole. Failure can impede mission assurance of associated services and can translate into failure to achieve organizational goals and objectives. Thus, ensuring the operational resilience of high-value assets is paramount to organizational success.

---

[6] In CERT-RMM, we take a ~~c~~yber" approach to resilience. That is, we specifically exclude considerations of other tangible, raw materials which are important to the delivery of some services and most manufacturing processes. This is not to say that physical materials cannot be considered in CERT-RMM, but explicit processes and practices for this are not included in the core model.

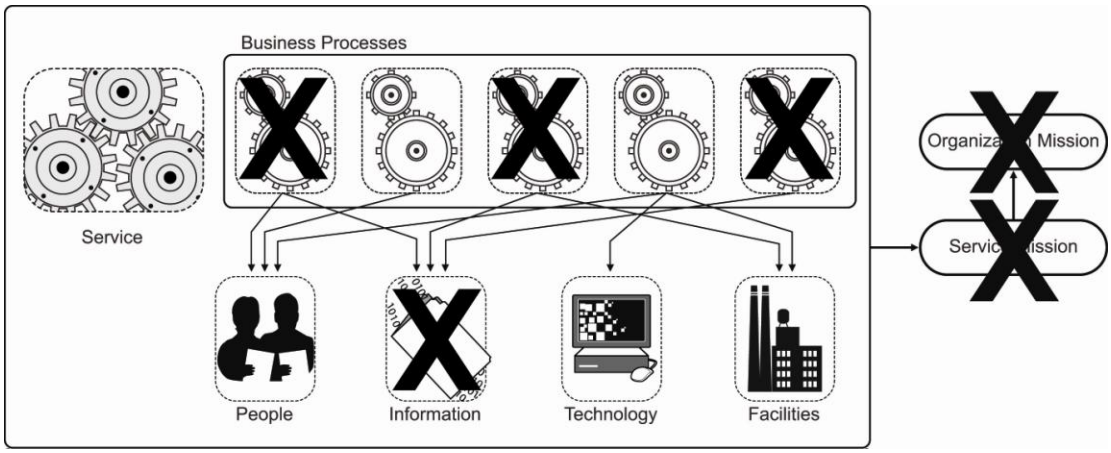


Figure 7: Impact of Disrupted Asset on Service Mission

The first step in establishing the operational resilience of assets is to identify and define the assets. Because assets derive their value and importance through their association with services, the organization must first determine which services are high-value. This provides structure and guidance for developing an inventory of high-value assets for which resilience requirements will need to be established and satisfied. Inventorying these assets is also essential to ensuring that changes are made in resilience requirements as operational and environmental changes occur.

Each type of asset for a specific service must be identified and inventoried. The following are descriptions of the four asset types used in CERT-RMM:

- People are those individuals who are vital to the expected operation and performance of the service. They execute the process and monitor it to ensure that it is achieving its mission, and make corrections to the process when necessary to bring it back on track. People may be internal or external to the organization.
- Information is any information or data, in paper or electronic form, that is vital to the intended operation of the service. Information may also be the output or byproduct of the execution of a service. Information can be as small as a bit or byte, a record or a file, or as large as a database. Because of confidentiality and privacy concerns, information must also be categorized as to its organizational sensitivity. Categorization provides another level of important description to an information asset that may affect its protection and continuity strategies. Examples of information include social security numbers, a vendor database, intellectual property, and institutional knowledge.
- Technology describes any technology component or asset that supports or automates a service and facilitates its ability to accomplish its mission. Technology has many layers, some of which are specific to a service (such as an application system) and others that are shared by the organization (such as the enterprise-wide network infrastructure) to support more than one service. Organizations must describe technology assets in terms that facilitate development and satisfaction of resilience requirements. In some organizations, this may be at the application system level; in others, it might be more granular, such as at the server or personal computer level. CERT-RMM characterizes technology assets as software, systems, or hardware. Technology assets can also include firmware and other assets including physical interconnections between these assets, such as cabling.

- Facilities are any physical plant assets that the organization relies upon to execute a service. Facilities are the places where services are executed and can be owned and controlled by the organization or by external business partners (referred to as external entities in the model). Facilities are often shared such that more than one service is executed in and dependent upon them. For example, a substantial number of services are executed inside of a headquarters office building. Facilities provide the physical space for the actions of people, the use and storage of information, and the operations of technology components. Thus, resilience planning for facilities must integrate tightly with planning for the other assets. Examples of facilities include office buildings, data centers, and other real estate where services are performed.

As shown in Figure 8, relationships among assets have implications for resilience. Information is the most "embedded" type of asset; its resilience is linked to the technologies in which it is developed, processed, stored, and transmitted as well as the facilities within which the technology physically resides.

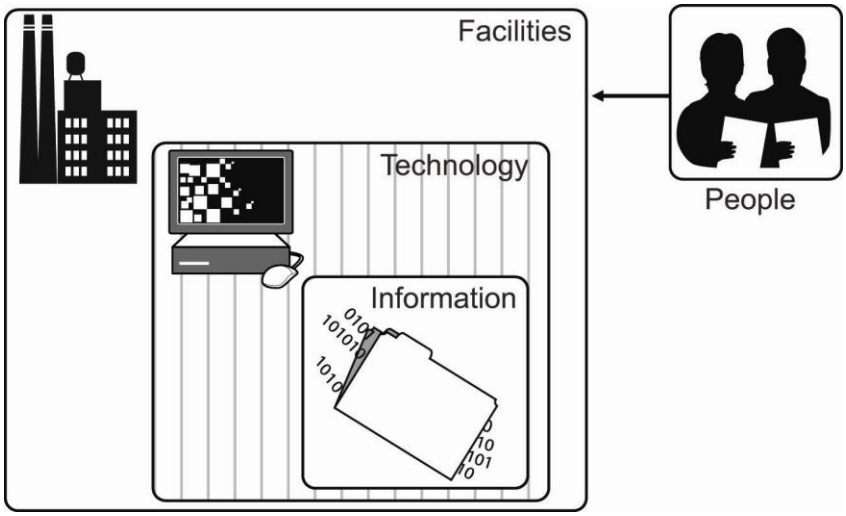


Figure 8: Putting Assets in Context

High-value assets have *owners* and *custodians*. Asset owners are the persons or organizational units, internal or external to the organization, that have primary responsibility for the viability, productivity, and resilience of the asset. For example, an information asset such as customer data may be owned by the customer relations department or the customer relationship manager. It is the owner's responsibility to ensure that the appropriate level of confidentiality, integrity, and availability requirements are defined and satisfied to keep the asset productive and viable for use in services.

Asset custodians are persons or organizational units, internal or external to the organization, who agree to and are responsible for implementing and managing controls to satisfy the resilience requirements of high-value assets while they are in their care. For example, the customer data in the above example may be stored on a server that is maintained by the IT department. In essence, the IT department takes custodial control of the customer data asset when the asset is in its domain. The IT department must commit to taking actions commensurate with satisfying the requirements for protection and continuity of the asset by its owners. However, in all cases,

owners are responsible for ensuring the proper protection and continuity of their assets, regardless of the actions (or inactions) of custodians.

2.2.4 Resilience Requirements

An operational resilience requirement is a constraint that the organization places on the productive capability of a high-value asset to ensure that it remains viable and sustainable when charged into production to support a high-value service. In practice, operational resilience requirements are a derivation of the traditionally described security objectives of confidentiality, integrity, and availability. Well known as descriptive properties of information assets, these objectives are also extensible to other types of assets—people, technology, and facilities—with which operational resilience management is concerned. For example, in the case of information, if the integrity requirement is compromised, the information may not be usable in the form intended, thus impacting associated business processes and services. Correspondingly, if unintended changes are made to the information (compromise of integrity), these may cause the business process or service to produce unintended results.

Resilience requirements provide the foundation for how assets are protected from threats and made sustainable so that they can perform as intended in support of services. Resilience requirements become a part of an asset's DNA (just like its definition, owner, and value) that transcends departmental and organizational boundaries because they stay with the asset regardless of where it is deployed or operated.

As shown in Figure 9, the resilience requirements development process requires the organization to establish resilience requirements at the enterprise, service, and asset levels based on organizational drivers, risk assumptions and tolerances, and resilience goals and objectives. Resilience requirements also drive or influence many of the processes that define operational resilience management. For example, resilience requirements form the basis for protect and sustain strategies. These strategies determine the type and level of controls needed to ensure operational resilience; conversely, controls must satisfy the requirements from which they derive.

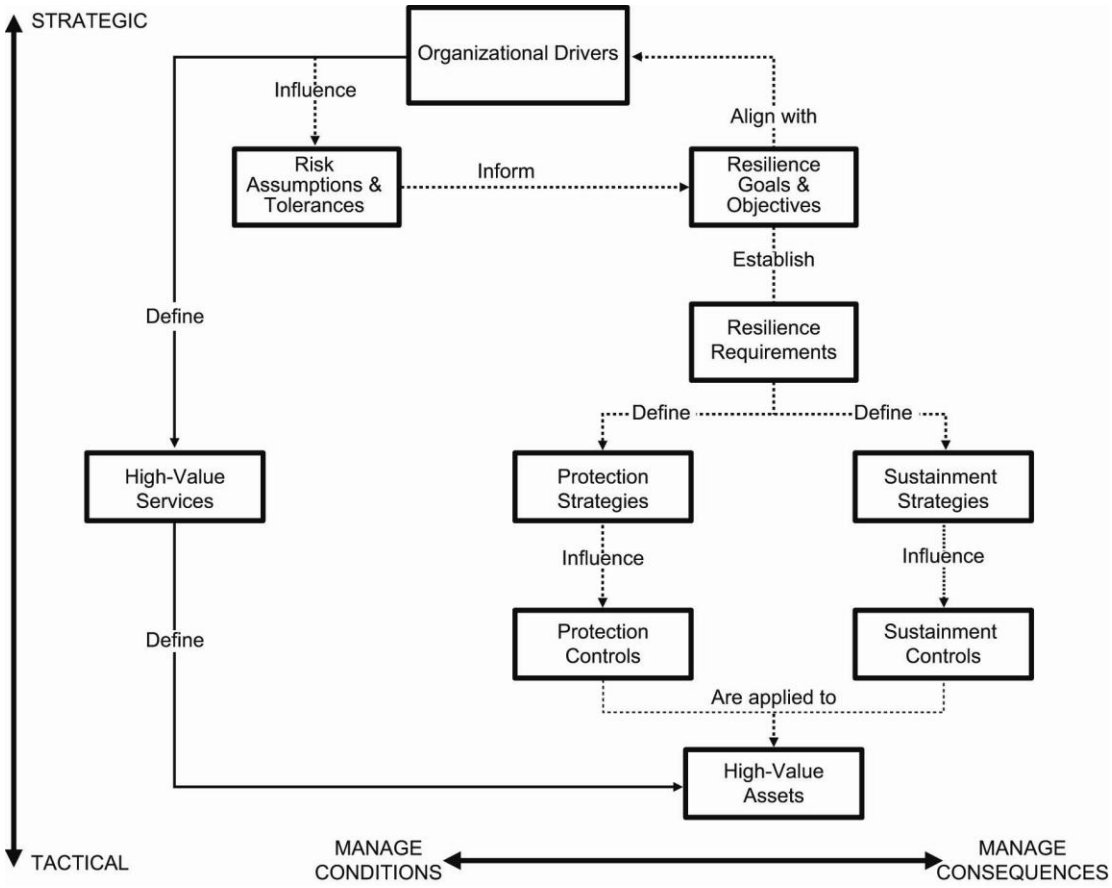


Figure 9: Driving Operational Resilience Through Requirements

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

2.2.5 Strategies for Protecting and Sustaining Assets

As discussed above, protect and sustain strategies are used to identify, develop, implement, and manage controls commensurate with an asset's resilience requirements. As the name implies, protect strategies are protective. They address how to minimize risks to the asset resulting from exposure to threats and vulnerabilities. Sustain strategies are focused on asset and service continuity. Such strategies define how to keep the asset operational when under stress and how to keep associated services operable when the asset is not available. Each asset needs an optimized mix of protect and sustain strategies.

Protect strategies translate into activities designed to minimize an asset's exposure to sources of disruption and to the exploitation of vulnerabilities. As shown in Figure 10, these strategies manage the conditions of risk by reducing threat and asset exposure. Such activities typically fall

into the "security" function but may also be embedded in IT operations processes. Activities that implement protect strategies often appear as processes, procedures, policies, and controls.

Sustain strategies translate into activities designed to keep assets operating as close to normal as possible when faced with disruptive, stressful events. These strategies aid in managing the consequences of risk by making consequences less likely and allowing the organization to respond more effectively to address consequences when an event occurs. Such activities typically fall into the "business continuity" function. Activities that implement sustain strategies often also appear as processes, procedures, policies, plans, and controls.

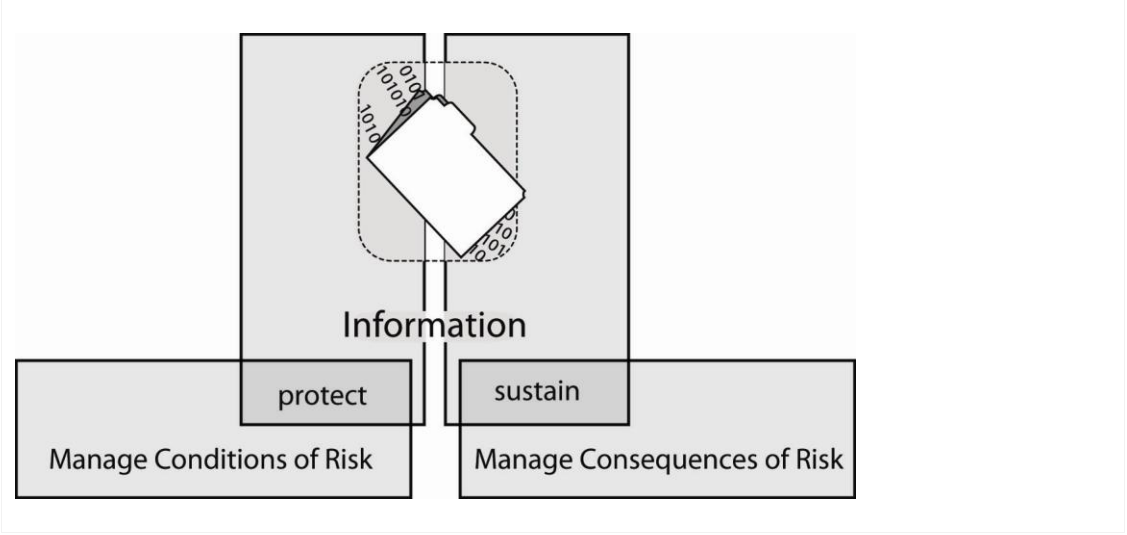


Figure 10: Optimizing Information Asset Resilience

The optimization of protect and sustain strategies and activities that minimize risk to assets and services while making efficient use of limited resources defines the management challenge of operational resilience.

2.2.6 Life-Cycle Coverage

Each of the assets covered in CERT-RMM has a life cycle. From a generic perspective, the majority of operational resilience management processes in CERT-RMM focus on the deployment and operation life-cycle phases, as shown in Figure 11.

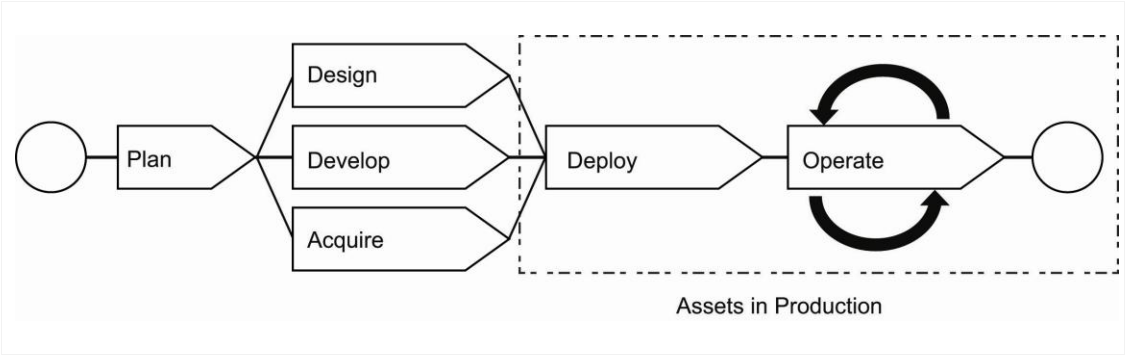


Figure 11: Generic Asset Life Cycle

However, some practices in CERT-RMM cover earlier life-cycle phases to ensure that operational resilience is considered during asset design and development, which can fortify an asset's defense against vulnerabilities and disruption in the operations phase. For example, the practices in Resilience Requirements Development and Resilience Requirements Management can be considered early life-cycle activities (in the plan, design, develop, and acquire phases) that address the development and management of resilience requirements early in the life of an asset.

Depending on the asset, the life-cycle treatment in CERT-RMM can appear to be inconsistent; however, model architects were purposeful in determining which early life-cycle activities to include in the model for maximum effectiveness in meeting operational resilience objectives.

The following briefly describes CERT-RMM life-cycle coverage for each asset type and for services.

People Life Cycle

People are hired, trained, and deployed in services. The activities of hiring and training staff, as well as determining their fitness for duty or purpose, are considered early life-cycle activities. Thus, some of the practices included in CERT-RMM address the hiring, training, and development of people. CERT-RMM also addresses the late life-cycle activity of decommissioning people deployed to services, which might include transfer, voluntary separation, or termination.

Information Life Cycle

Information is created or developed, used by people and services, and then disposed of at the end of its useful life. CERT-RMM practices address the early life-cycle activities related to the development and management of information resilience requirements, the development and implementation of respective controls to meet the requirements, the secure and sustainable use of the information, and the secure disposition of the information. Thus CERT-RMM covers the entire information life cycle.

Technology Life Cycle

Technology is most closely defined by traditional life-cycle descriptions. Software, systems, and hardware are planned, designed, developed or acquired, implemented, and operated. For the most part, CERT-RMM focuses on the operations phase of the life cycle for technology assets. However, process areas such as Controls Management address the early consideration of controls that need to be designed into software and systems. And the Resilient Technical Solution Engineering process area provides a useful process definition for managing the consideration and inclusion of resilience quality attributes into software and systems throughout their development life cycle. Correspondingly, the External Dependencies Management process area includes these same considerations when software and systems are being acquired.

Figure 12 depicts the reach back into earlier life-cycle phases for these categories of technology assets.

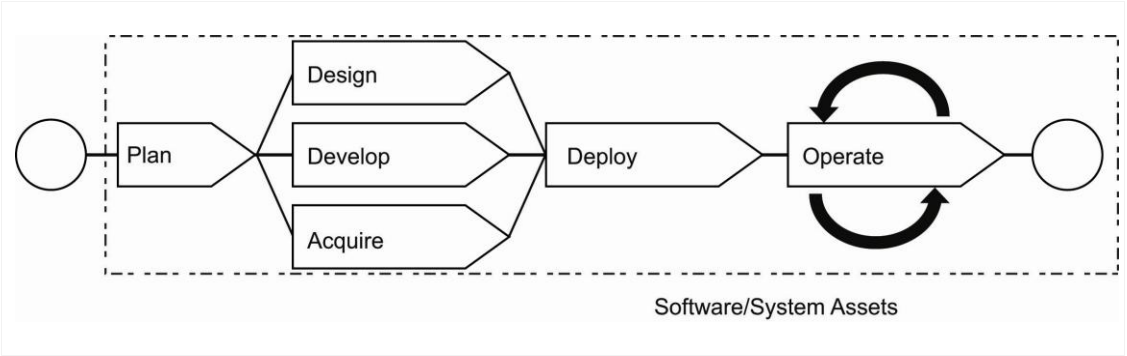


Figure 12: Software/System Asset Life Cycle

Facilities Life Cycle

Facilities are planned, designed, developed or acquired, constructed, and operated, and then retired at the end of their useful life. CERT-RMM practices address early life-cycle activities of developing and managing resilience requirements for facilities, for developing, implementing and managing physical facilities controls, for maintaining the vital physical and electronic systems of the facility, and for the closure or disposition of the facility.

Services Life Cycle

For services, operational resilience management processes primarily focus on the deployment and operation phases of a service's life cycle[7] as shown in Figure 13.

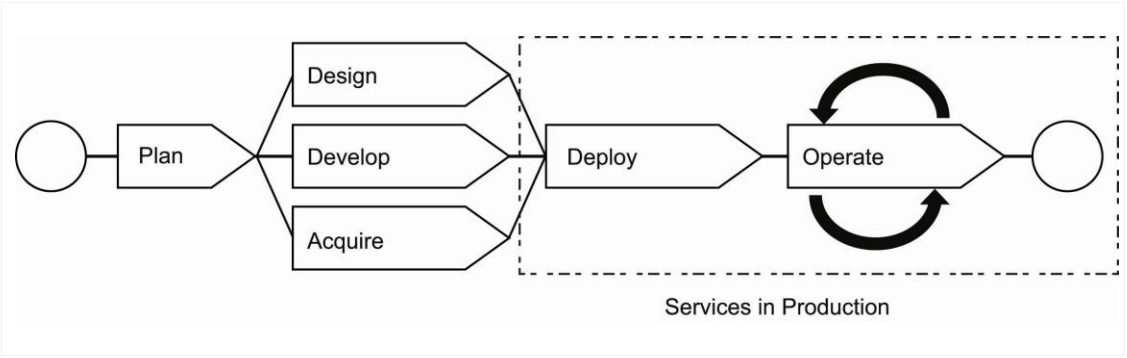


Figure 13: Services Life Cycle

At a high level in CERT-RMM, services are identified, prioritized, and communicated as the basis for organizational success. Service profiles and attributes are kept up-to-date in an accessible service repository. Assets (as defined above) associated with or used by each service are identified and kept current as are interdependencies between services and business processes.

From a model perspective, the processes defined in CERT-RMM mostly act on the service while it is in operation to ensure that it can meet its mission consistently over time. However, some early life-cycle activities for services are included in CERT-RMM. For example, the resilience

[7] The early life-cycle activities for services (design, development, and implementation) are covered in the CMMI for Services model. CERT-RMM addresses services in operation as they support the achievement of organizational goals and objectives.

requirements for services are defined and managed in Resilience Requirements Definition and Resilience Requirements Management, respectively. Through the lens of associated assets, the resilience attributes for the service are identified in these processes and carried out through other processes such as Controls Management and Service Continuity. When controls and service continuity plans are established, these processes can be considered early life cycle; conversely, when controls and service continuity plans are implemented and managed, these processes are considered to be in the operations phase of the life cycle for services.

In addition, changing conditions that affect services in the operations phase are reflected in changes to controls and service continuity plans. These conditions include

- changes in a service's or asset's resilience requirements
- identification of new vulnerabilities, threats, and risks
- asset changes, such as staff changes, changes to information assets and technology, and relocation of facilities
- changes in a service's or asset's protective controls
- changes in the plan's stakeholders, including external entities and public agencies
- organizational changes, including staff and geographic changes
- changes in lines of business, industry, or product or services mix
- significant technical infrastructure changes
- changes in relationships with external entities such as vendors and business partners
- changes in or additions to regulatory or legal obligations
- results of service continuity plan execution
- results of service continuity plan testing

Other CERT-RMM Life Cycles

Other life cycles are also addressed in CERT-RMM. For example, the incident life cycle is the focus of the Incident Management and Control process area. In addition, service continuity as defined in the Service Continuity process area defines a life cycle for creating a service continuity program and planning, developing, testing, and executing service continuity plans.

2.3 Adapting CERT-RMM Terminology and Concepts

Organizations adopting the CERT-RMM may decide to replace some of the terminology used in these key concepts with whatever is comfortable, familiar, and useful to them. However, users of CERT-RMM are strongly encouraged to interpret and apply the foundational concepts (disruption and stress, convergence, operational resilience) and the elements of operational resilience (services, business processes, assets, and resilience requirements, strategies to protect and sustain, and life-cycle coverage) to gain the benefits of managing and improving operational resilience using the model.

3 Model Components

This chapter introduces the CERT-RMM process areas and their categories and describes the process area components and their categories. You will need to fully understand this information to make use of the process areas contained in Part Three. It may be helpful to skim a few process areas before you read this section to become familiar with their general construction and layout.

3.1 The Process Areas and Their Categories

As in CMMI models, a process area in the CERT-RMM is "a cluster of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making improvement in that area" [CMMI Product Team 2009, pg. 10]. The CERT-RMM has 26 process areas (PAs) that are organized into high-level operational resilience categories: Engineering, Enterprise Management, Operations, and Process Management. Table 3 shows the 26 CERT-RMM process areas by category.

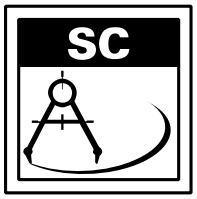
Table 3: Process Areas by Category

Category	Process Area
Engineering	Asset Definition and Management
Engineering	Controls Management
Engineering	Resilience Requirements Development
Engineering	Resilience Requirements Management
Engineering	Resilient Technical Solution Engineering
Engineering	Service Continuity
Enterprise Management	Communications
Enterprise Management	Compliance
Enterprise Management	Enterprise Focus
Enterprise Management	Financial Resource Management
Enterprise Management	Human Resource Management
Enterprise Management	Organizational Training and Awareness
Enterprise Management	Risk Management
Operations	Access Management
Operations	Environmental Control
Operations	External Dependencies Management
Operations	Identity Management
Operations	Incident Management and Control
Operations	Knowledge and Information Management
Operations	People Management
Operations	Technology Management
Operations	Vulnerability Analysis and Resolution
Process Management	Measurement and Analysis
Process Management	Monitoring
Process Management	Organizational Process Definition
Process Management	Organizational Process Focus

Categories are further elaborated and described in Section 4.1.

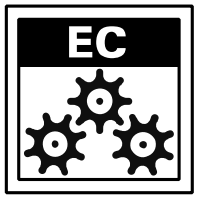
3.1.1 Process Area Icons

The process area categories are reinforced visually in the model by process area icons. The process area icons show the process area tags (explained below and in Section 3.4) and the symbol of the process area's operational resilience management area. Figure 14 shows an example of a process area icon from each operational resilience management area.

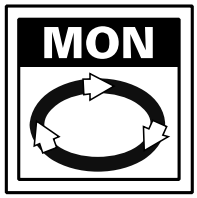


Service Continuity Process Area
Engineering category

Communications Process Area
Enterprise management category



Environmental Control Process Area
Operations category



Monitoring Process Area
Process management category

Figure 14: Examples of Process Area Icons

3.2 Process Area Component Categories

CERT-RMM process areas contain three categories of components: Required, Expected, and Informative. These categories provide an aid in establishing process improvement objectives and in adapting the model to an organization's unique circumstances.[8]

Table 4 lists the model components in each category.

[8] Much of the nomenclature used in CERT-RMM is derived from CMMI. Thus, if you are already familiar with CMMI models, you should notice no differences in the way that these components are defined or used.

Table 4: CERT-RMM Components by Category

Required	Expected	Informative
specific goal statements	specific practice statements	purpose statements
generic goal statements	generic practice statements	introductory notes
		related process areas section
		summary of specific goals and practices
		goal and practice titles
		typical work products
		subpractices
		notes
		example blocks
		generic practice elaborations
		references
		amplifications

3.2.1 Required Components

Required components describe what an organization must achieve to satisfy a process area. There are two required components in CERT-RMM: *specific goal statements* and *generic goal statements*. Goal satisfaction is used in CERT-RMM-based capability appraisals in determining capability levels (see Part Two, Section 6.4). Satisfaction of a goal means that it is visibly and verifiably implemented in the organization's processes.

Note that it is the goal *statements* that are required components, not the goal titles. The goal name of specific goal 1 in Asset Definition and Management is "Establish Organizational Assets"; the goal name of generic goal 1 is "Achieve Specific Goals."

3.2.2 Expected Components

Expected components describe the practices that an organization will typically implement to achieve required components. *Specific practice statements* and *generic practice statements* are both expected components in CERT-RMM. To satisfy goals, the specific and generic practices are expected to be present in the planned and implemented processes of the organization unless acceptable alternatives are present.

Again, note that it is the practice *statements* that are expected components, not the practice titles.

3.2.3 Informative Components

Informative components provide guidance and suggestions about how to achieve the required and expected components. The informative components in CERT-RMM are listed in Table 4.

For example, "Identify organizationally high-value services" is a subpractice in Asset Definition and Management specific practice 1 of specific goal 2, and "List of organizationally high-value services and associated assets" is a typical work product.

3.3 Process Area Component Descriptions

3.3.1 Purpose Statements

Purpose statements summarize the content of the process area and collectively represent the goals of the process area. For example, the purpose statement of the Service Continuity process area is "The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets in the event of an incident or disaster."

3.3.2 Introductory Notes

The introductory notes provide explanatory matter on the contents of the process area. They are designed to explain the scope of the process area and how developing competency in that area is important to achieving and sustaining resilience. Unique conditions or terminology are included in the introductory notes, as well as a summarization of the goals of the process area.

3.3.3 Related Process Areas Section

The related process areas section lists references to other process areas and reflects the high-level relationships among capabilities. This information is useful in deciding which other capabilities are complementary and should be considered by the organization when improving capability.

The following are two examples of relationships from the Service Continuity process area:

> *The identification of vital records and databases for service continuity is addressed in the Knowledge and Information Management process area.*
>
> *The consideration of consequences as a foundational element for developing service continuity plans is addressed in the Risk Management process area.*

3.3.4 Summary of Specific Goals and Practices

The summary of specific goals and practices is a table that lists the tag and title of all of the specific goals in the process area and the tag and title of the specific practices of each specific goal.

3.3.5 Specific Goals and Practices

The specific goals of each process area state at a high level the unique capabilities that characterize the process and are required for improving the process. They describe *what* to do to achieve the capabilities. Specific goals are decomposed into specific practices, which are considered to be the base practices that reflect the process area's body of knowledge. Specific practices are expected components of the process area that, when achieved, should promote accomplishment of the associated goal. They begin to articulate *how* to achieve process capabilities. Specific practices provide suggested ways to meet their associated goals, but in implementation they may differ from organization to organization.

Figure 15 shows a specific goal from the Asset Definition and Management process area with its required component, the specific goal statement.

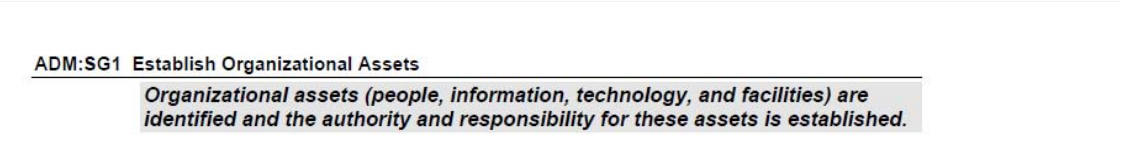


Figure 15: A Specific Goal and Specific Goal Statement

Figure 16 shows a specific practice from the Asset Definition and Management process area with its expected component, the specific practice statement.

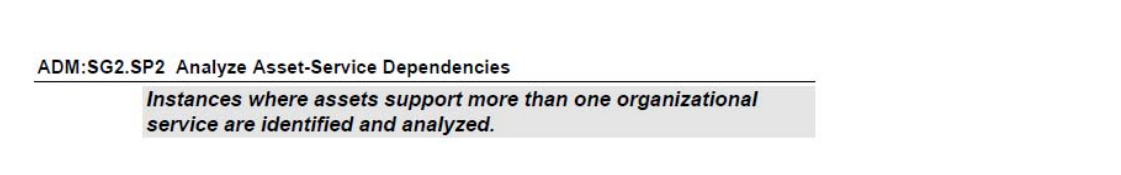


Figure 16: A Specific Practice and Specific Practice Statement

3.3.6 Generic Goals and Practices

Generic goals are called "generic" because the same goal statement applies to multiple process areas. A generic goal describes the capabilities that must be present to institutionalize the processes that implement a process area. A generic goal is a required model component and is used in appraisals to determine whether a process area is satisfied.

Figure 17 shows a generic goal from the Asset Definition and Management process area with its required component, the generic goal statement.

Figure 17: A Generic Goal and Generic Goal Statement

Generic practices are called "generic" because the same practice applies to multiple process areas. A generic practice is the description of an activity that is considered important in achieving the associated generic goal. (See Part Two, Chapter 5 for a more detailed description of generic goals and practices.)

Figure 18 shows a generic practice from the Asset Definition and Management process area with its expected component, the generic practice statement.

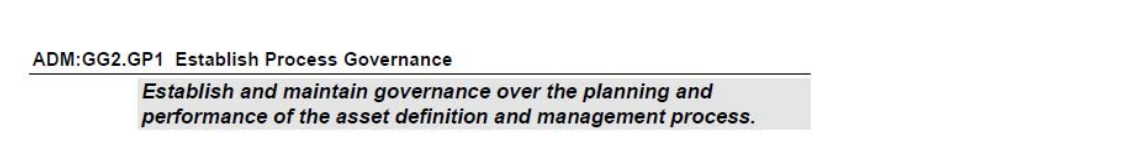


Figure 18: A Generic Practice and Generic Practice Statement

3.3.7 Typical Work Products

Typical work products describe the artifacts typically produced by a specific practice. As informative elements, these artifacts are not set in stone; rather, they are suggested from experience, and an organization may have similar or additional artifacts. Typical process artifacts are useful as model elements because they provide a baseline from which measurement of the performance of the practice can be gauged.

3.3.8 Subpractices, Notes, Example Blocks, Generic Practice Elaborations, References, and Amplifications

Subpractices are informative elements associated with each specific practice and relevant to typical work products. Subpractices are a transition point for process area specific practices because the focus changes at this point from *what* must be done to *how*. While not prescriptive or detailed, subpractices can help organizations determine how they can satisfy the specific practices and achieve the goals of the process area. Each organization will have its own subpractices that it has either organically developed or has acquired from a code of practice.

Subpractices can include notes and example blocks. Notes provide expanded and explanatory detail for subpractices where necessary. Examples provide relevant and real-world illustrations and depictions that support understanding of the subpractices.

Generic practice and subpractice elaborations provide guidance about how the generic practice should be applied uniquely to the process area. For example, in every process area, subpractice 1 of generic goal 2, generic practice 3 ("Provide Resources") is "Staff the process." In the Incident Management and Control process area, the subpractice elaboration lists examples of staff required to perform the incident management and control process, such as staff responsible for triaging events.

References are pointers to related, additional, or more detailed information in other process areas or other components within the same process area. The CERT-RMM *Code of Practice Crosswalk* [REF Team 2008b] contains subpractice references to common codes of practice that aid in effectively adopting CERT-RMM regardless of what practices an organization has already invested in and implemented.

Amplifications explain or describe a unique aspect of a practice. They are used in Asset Definition and Management to describe the differences between asset types. Otherwise, they are infrequently used in the current version of the model. Future versions of the model will use amplifications to describe how a particular process area is addressed for a specific asset type, such as software, systems, or facilities.

Figure 19 illustrates the structure of the major model components and indicates whether all or part of each component is required, expected, or informative.

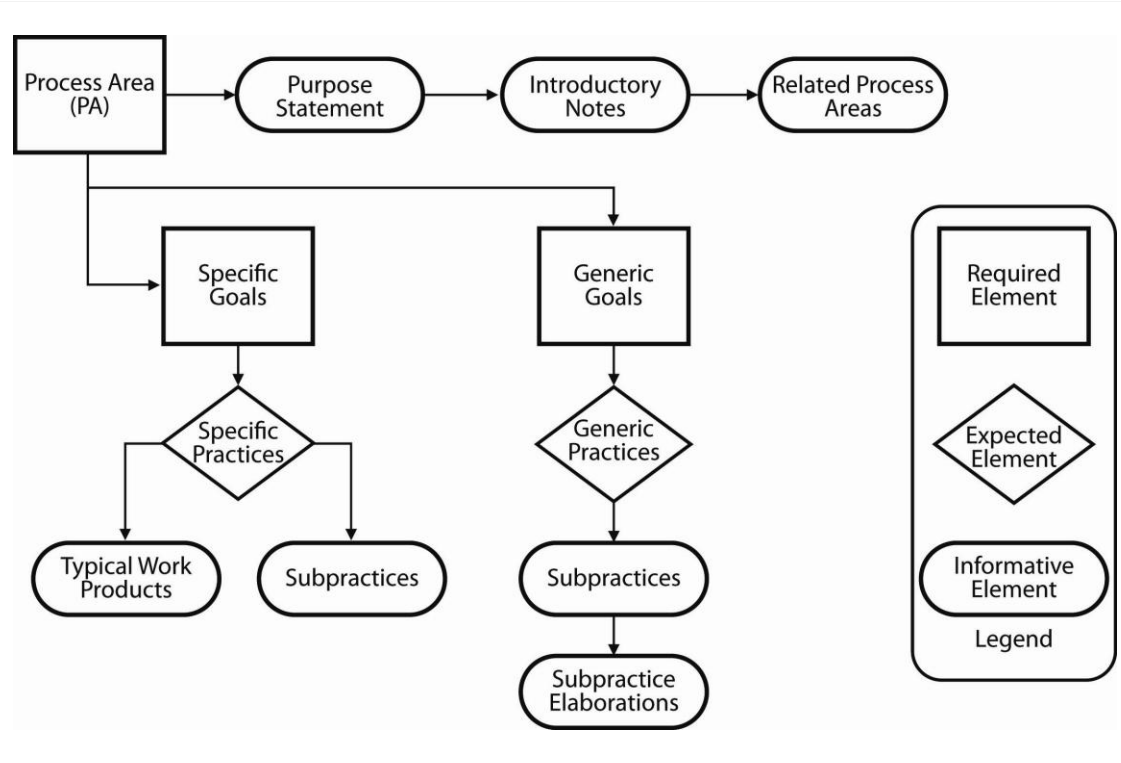


Figure 19: Summary of Major Model Components

3.4 Numbering Scheme

Process areas in CERT-RMM are tagged by a three- or four-letter tag. The tags for all the process areas are shown in Table 5.

Table 5: Process Area Tags

Process Area	Tag
Asset Definition and Management	ADM
Access Management	AM
Communications	COMM
Compliance	COMP
Controls Management	CTRL
Environmental Control	EC
Enterprise Focus	EF
External Dependencies Management	EXD
Financial Resource Management	FRM
Human Resource Management	HRM
Identity Management	ID
Incident Management and Control	IMC
Knowledge and Information Management	KIM
Measurement and Analysis	MA
Monitoring	MON
Organizational Process Definition	OPD
Organizational Process Focus	OPF

Process Area	Tag
Organizational Training and Awareness	OTA
People Management	PM
Risk Management	RISK
Resilience Requirements Development	RRD
Resilience Requirements Management	RRM
Resilient Technical Solution Engineering	RTSE
Service Continuity	SC
Technology Management	TM
Vulnerability Analysis and Resolution	VAR

Specific and generic goals are tagged and numbered as follows: SG refers to a specific goal; GG refers to a generic goal. These are appended to the CERT-RMM process area tags and numbered. For example, "ADM:SG1" is specific goal 1 in the Asset Definition and Management process area, and "ADM:GG3" is generic goal 3 in the Asset Definition and Management process area.

Specific and generic practices are tagged and numbered as follows: SP refers to a specific practice; GP refers to a generic practice. These are appended to the CERT-RMM process area tags and the specific goal and generic goal tags respectively and are numbered. For example, "ADM:SG1.SP1" is specific practice 1 in specific goal 1 in ADM, and "ADM:GG2.GP3" is generic practice 3 in generic goal 2 in ADM.

Typical work products are numbered sequentially beginning with "1" within each specific practice. Subpractices are numbered sequentially beginning with "1" in each specific or generic practice. Subpractices are referenced in text with their specific or generic practice tag. For example, "ADM:SG2.SP1 subpractice 1" is subpractice 1 in specific practice 1 in specific goal 2 in ADM, and "ADM:GG2.GP3 subpractice 2" is subpractice 2 in generic practice 3 in generic goal 2 in ADM.

3.5 Typographical and Structural Conventions

Typographical and structural conventions have been used in the model to distinguish model components and make them easier to recognize. Also, references to other process areas or process area components are always styled in italic in the RMM.

These conventions can be seen in Figure 20, which shows extracts of process area pages with model components identified.

Figure 20: Format of Model Components

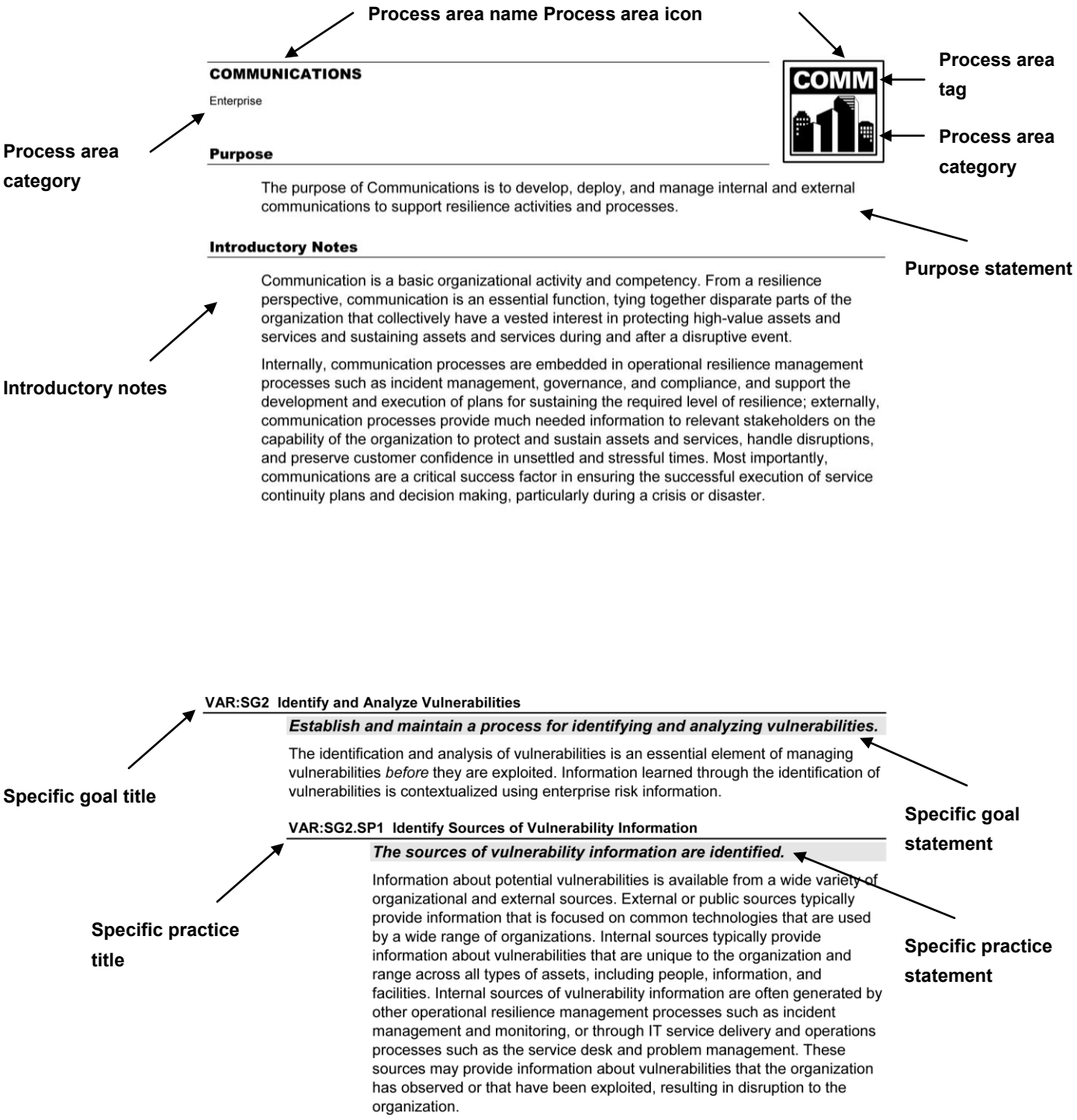
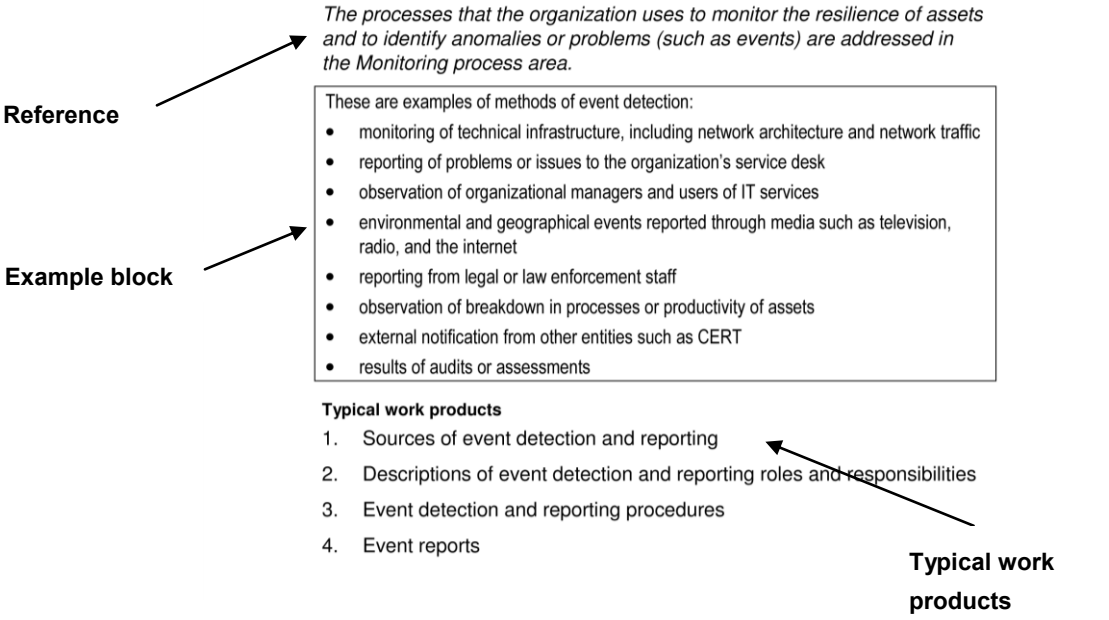


Figure 20, continued



The processes that the organization uses to monitor the resilience of assets and to identify anomalies or problems (such as events) are addressed in the Monitoring process area.

These are examples of methods of event detection:

- monitoring of technical infrastructure, including network architecture and network traffic
- reporting of problems or issues to the organization's service desk
- observation of organizational managers and users of IT services
- environmental and geographical events reported through media such as television, radio, and the internet
- reporting from legal or law enforcement staff
- observation of breakdown in processes or productivity of assets
- external notification from other entities such as CERT
- results of audits or assessments

Typical work products

1. Sources of event detection and reporting
2. Descriptions of event detection and reporting roles and responsibilities
3. Event detection and reporting procedures
4. Event reports

Subpractices

1. Define the methods of event detection and reporting.
2. Develop and communicate descriptions of event detection and reporting roles and responsibilities *(refer to IMC:SG1.SP1)*.
3. Assign the roles of event detection and reporting to appropriate staff throughout the organization *(refer to IMC:SG1.SP2)*.

   Ensure that those assigned the responsibility for event detection and reporting understand this responsibility and have committed to performing it.
4. Establish a process for event reporting. Document events as they are detected on an event report.

2. Fund the process.

   Elaboration:

   In the case of incident management and control, funding must extend to supporting the incident life cycle and considerations must be made for unknown funding requirements related to incident management that are relative to the type and extent of incident and the impact on the organization. Extending consideration to these unpredictable needs provides the organization a level of control over unplanned and potentially unconstrained costs.

4 Model Relationships

Successful process improvement efforts align with and help to accomplish business and strategic objectives. Otherwise, there is no reason for the organization to invest in improving processes. Business and strategic objectives may either reflect the organization's critical success factors (to improve sales volume), compliance regulations (to meet stricter information privacy rules), or even to address a continuing issue or challenge for the organization (to prevent further data breaches). These objectives should drive how you use model-based process improvement methods, techniques, and tools, including CERT-RMM.

CERT-RMM in its entirety looks ominous at first glance. One reason for this is that operational resilience management encompasses many disciplines and practices. Another reason is that CERT-RMM provides extensive elaborative material to help you make practical use of the model. Once you understand the relationships in the model—and you are able to connect these with your own operational resilience management processes—the CERT-RMM processes that are most relevant to you will be fairly easy to identify and adopt.

There are two types of relationships that are useful to understand as you become familiar with the model. The *model view* helps you to understand the model from an architectural perspective. The way that process areas are grouped provides perspective on the area of operational resilience management that those process areas are intended to support. The *objective view* helps you see the model through relationships that support a particular objective and what you want to accomplish. For example, if your objective is to improve the management of vulnerabilities to high-value information assets, the objective view links together the process areas that would satisfy this objective. Because CERT-RMM allows you to develop an approach to improvement that addresses specific objectives, understanding each of these types of relationships can also be important in helping you develop meaningful targeted improvement roadmaps, as discussed in Section 6.3.

Understanding the key relationships that exist among CERT-RMM process areas aids your adoption and application of the model. For this reason, each process area references other process areas, and details the nature of the relationships between them. These references can be found in the "Related Process Areas" section of each process area in Part Three.

In this section we describe the model views and provide two visual examples of how CERT-RMM process areas relate to each other to accomplish a common objective. As the model continues to be used and adopted, additional objectives and relationships will be developed and described.

4.1 The Model View

The model view simply arranges the process areas by process category. Process areas in each category share common characteristics that form the foundational architecture of the model.

4.1.1 Enterprise Management

The enterprise is an important concept in managing operational resilience. At the enterprise level, the organization establishes and carries out many activities that set the tone for operational resilience, such as governance, risk management, and financial responsibility.

The process areas in the Enterprise Management category represent functions and activities that are essential to broadly supporting the operational resilience management process. This does not mean that these processes are or need to be functionally positioned at an enterprise level. Instead, they represent organization-wide competencies that affect the operational resilience of organizational units. For example, the practices in the Risk Management process area may be performed by an organizational unit, but their effectiveness may be limited by the overall risk management capability of the organization.

The process areas that represent the Enterprise Management category are

- Communications [COMM]
- Compliance Management [COMP]
- Enterprise Focus [EF]
- Financial Resource Management [FRM]
- Human Resource Management [HRM]
- Organizational Training and Awareness [OTA]
- Risk Management [RISK]

Figure 21 depicts the relationships that drive resilience activities at the enterprise level.

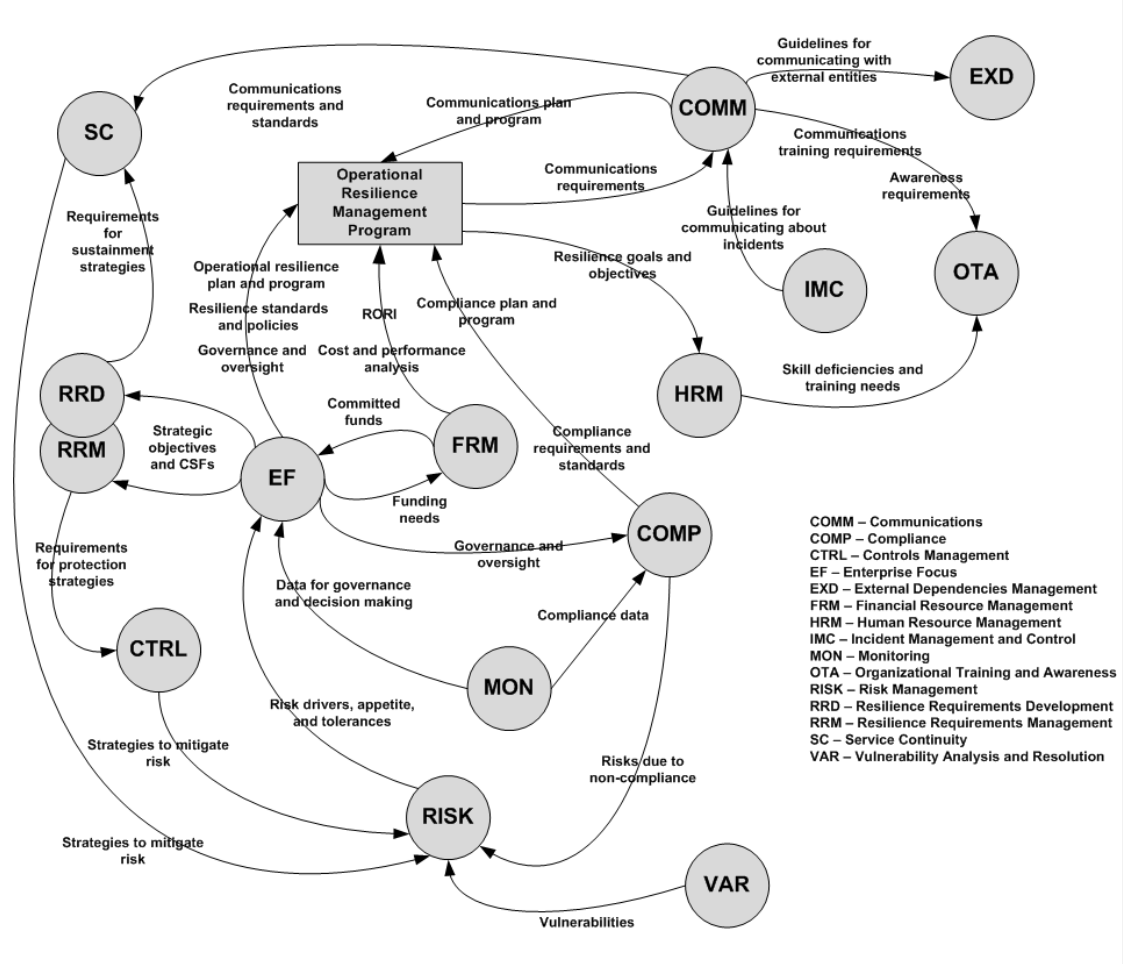


Figure 21: Relationships That Drive Resilience Activities at the Enterprise Level

Engineering

Aspects of operational resilience management are requirements-driven. Thus, the process areas in the Engineering category represent those that are focused on establishing and implementing resilience for organizational assets, business processes, and services through a requirements-driven process. These processes establish the basic building blocks for resilience and create the foundation to protect and sustain assets and, by reference, the business processes and services that assets support.

Engineering process areas fall into three broad categories:

- *Requirements Management* addresses the development and management of the security (protect) and resilience (sustain) objectives for assets and services.
- *Asset Management* establishes the important people, information, technology, and facilities assets across the enterprise.
- *Establishing and Managing Resilience* addresses the selection, implementation, and management of preventive controls and the development and implementation of service continuity and impact management plans and programs. It also addresses early life cycle consideration of resilience quality attributes for software and systems.

The Engineering process areas include

Requirements Management

- Resilience Requirements Development [RRD]
- Resilience Requirements Management [RRM]

Asset Management

- Asset Definition and Management [ADM]

Establishing and Managing Resilience

- Controls Management [CTRL]
- Resilient Technical Solution Engineering [RTSE]
- Service Continuity [SC]

Operations

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

Operations process areas fall into three broad categories:

- *Supplier Management* addresses the management of external dependencies and the potential impact on the organization's operational resilience.
- *Threat, Vulnerability, and Incident Management* addresses the organization's continuous cycle of identifying and managing threats, vulnerabilities, and incidents to minimize organizational disruption.
- *Asset Resilience Management* addresses the asset-level activities that the organization performs to manage operational resilience of people, information, technology, and facilities to ensure business processes and services are sustained.

The Operations process areas are

Supplier Management

- External Dependency Management [EXD]

Threat and Incident Management

- Access Management [AM]
- Identity Management [ID]
- Incident Management and Control [IMC]
- Vulnerability Analysis and Resolution [VAR]

Asset Resilience Management

- Environmental Control [EC]
- Knowledge and Information Management [KIM]
- People Management [PM]
- Technology Management [TM]

Figure 22 depicts the relationships that drive threat and incident management.

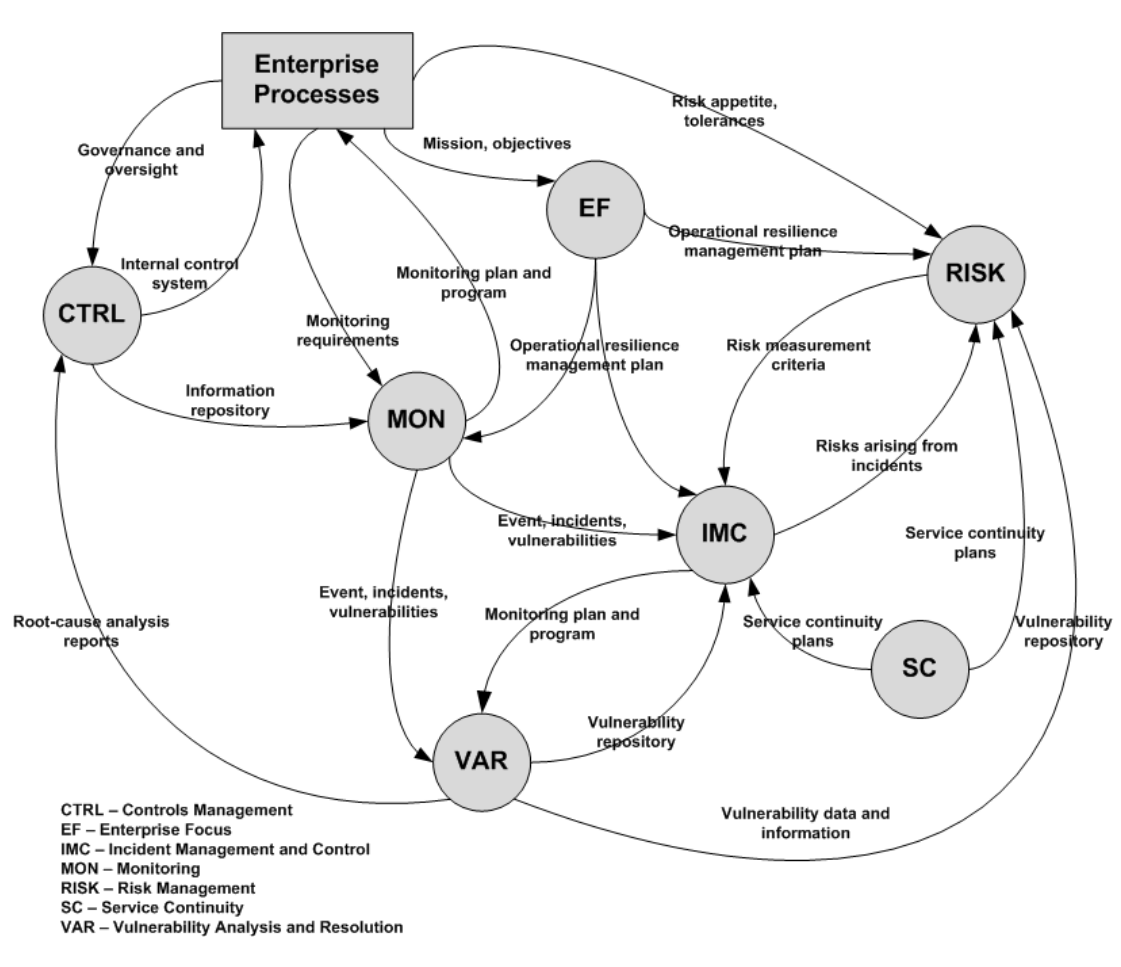


Figure 22: Relationships That Drive Threat and Incident Management

Process Management

Process Management processes represent those that are focused on measuring, managing, and improving the operational resilience management process. These process areas represent the extension of process improvement concepts to operational resilience management and, in turn, to the disciplines of security and business continuity. Process areas in this category are intended to catalyze the organization's view of resilience as a repeatable, predictable, manageable, and improvable process over which it has a significant level of active and direct control.

Process Management process areas can be expressed by two broad categories:

- *Data Collection and Logging* addresses the organization's competencies for identifying, collecting, logging, and disseminating information needed to ensure that operational resilience management processes are performed consistently and within acceptable tolerances.
- *Process Management* addresses the activities the organization performs to improve and optimize operational resilience management processes and to make these processes consistent throughout the organization.

Process Management process areas are

Data Collection and Logging

- Monitoring [MON]

Process Management

- Organizational Process Definition [OPD]
- Organizational Process Focus [OPF]
- Measurement and Analysis [MA]

4.2 Objective Views for Assets

Objective views in CERT-RMM can address a number of useful perspectives, such as

- how operational resilience management is planned and executed
- the specific processes that drive asset-based resilience, such as relationships that drive information resilience
- how people are addressed in operational resilience management
- the development and deployment of protection strategies and controls
- the service continuity planning process

With a large model, the number of possible objective views could be significant and would be beyond the scope of this report. A basic set of objective views can address the operational resilience management of the assets that are the focus of the model. The following describes these views and provides four figures that graphically depict model objectives.

People

Figure 23 shows the CERT-RMM process areas that participate in managing the operational resilience of people. They establish people as an important asset in service delivery and ensure that people meet job requirements and standards, have appropriate skills, are appropriately trained, and have access to other assets as needed to do their jobs.

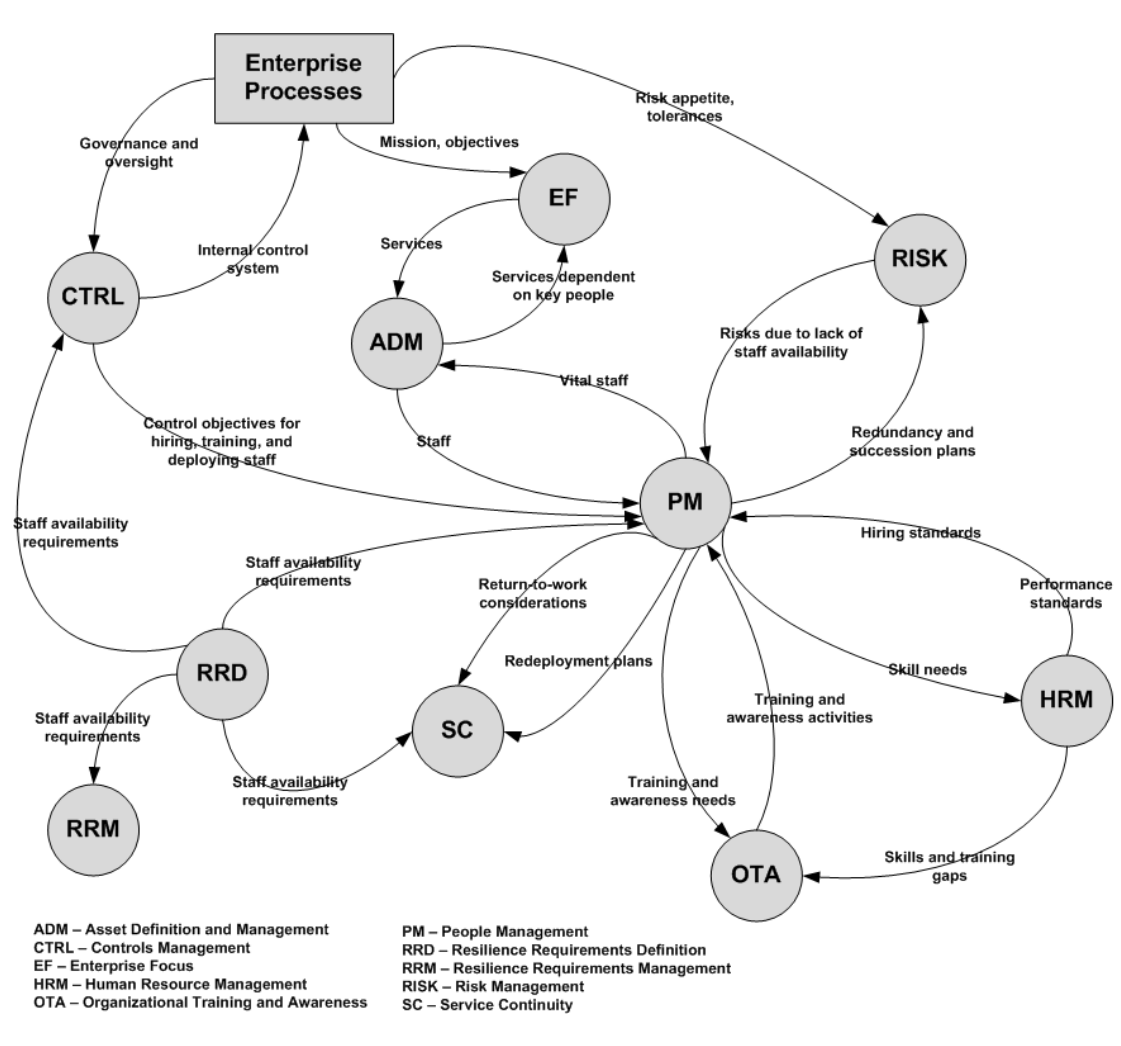


Figure 23: Relationships That Drive the Resilience of People

Information

Figure 24 shows the CERT-RMM process areas that drive the operational resilience management of information. Information is established as a key element in service delivery. Requirements for protecting and sustaining information are established and utilized by processes such as risk management, controls management, and service continuity planning.

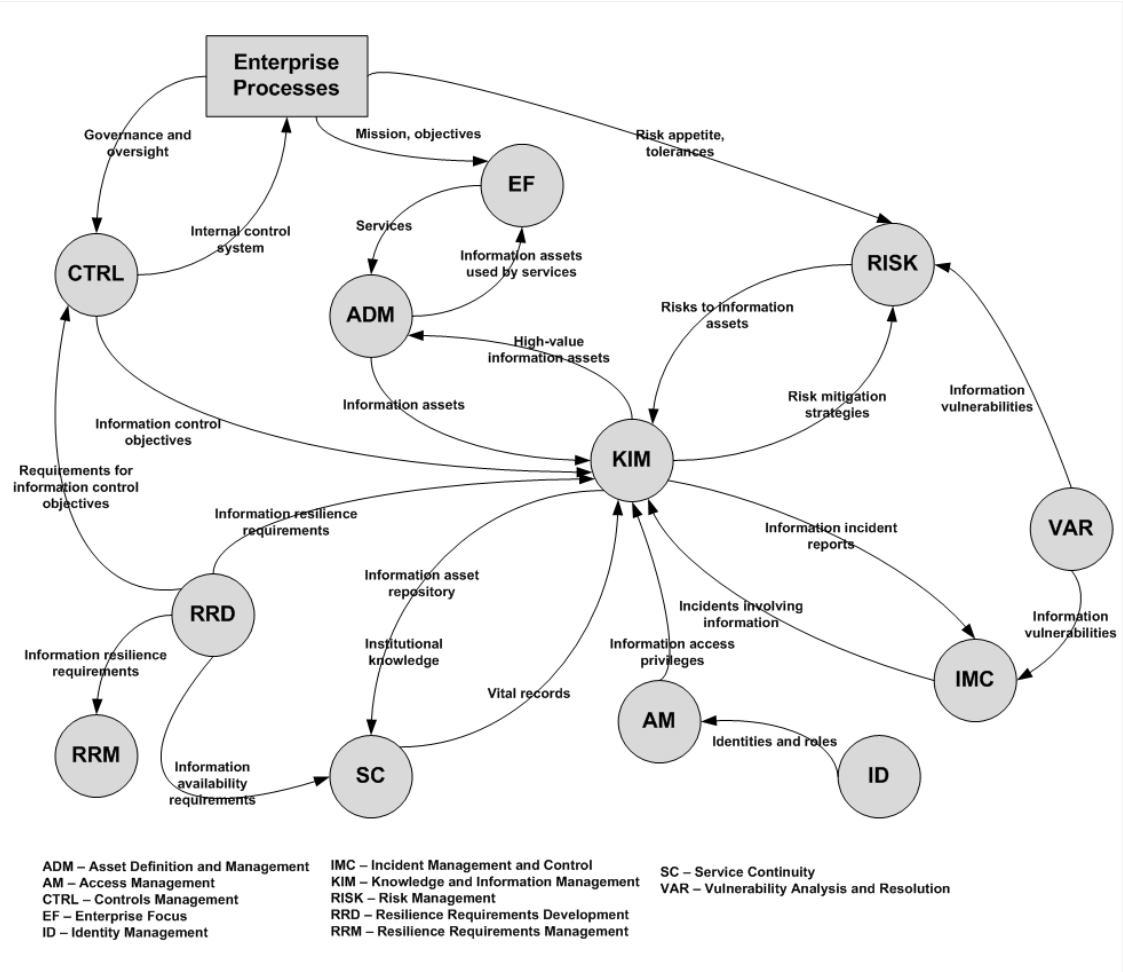


Figure 24: Relationships That Drive Information Resilience

Technology

Figure 25 shows the CERT-RMM process areas that drive the operational resilience management of technology. These relationships address the specific complexities of software and systems resilience, as well as the resilience of architectures where the technology assets reside, development and acquisition processes, and processes such as configuration management and capacity planning and management.

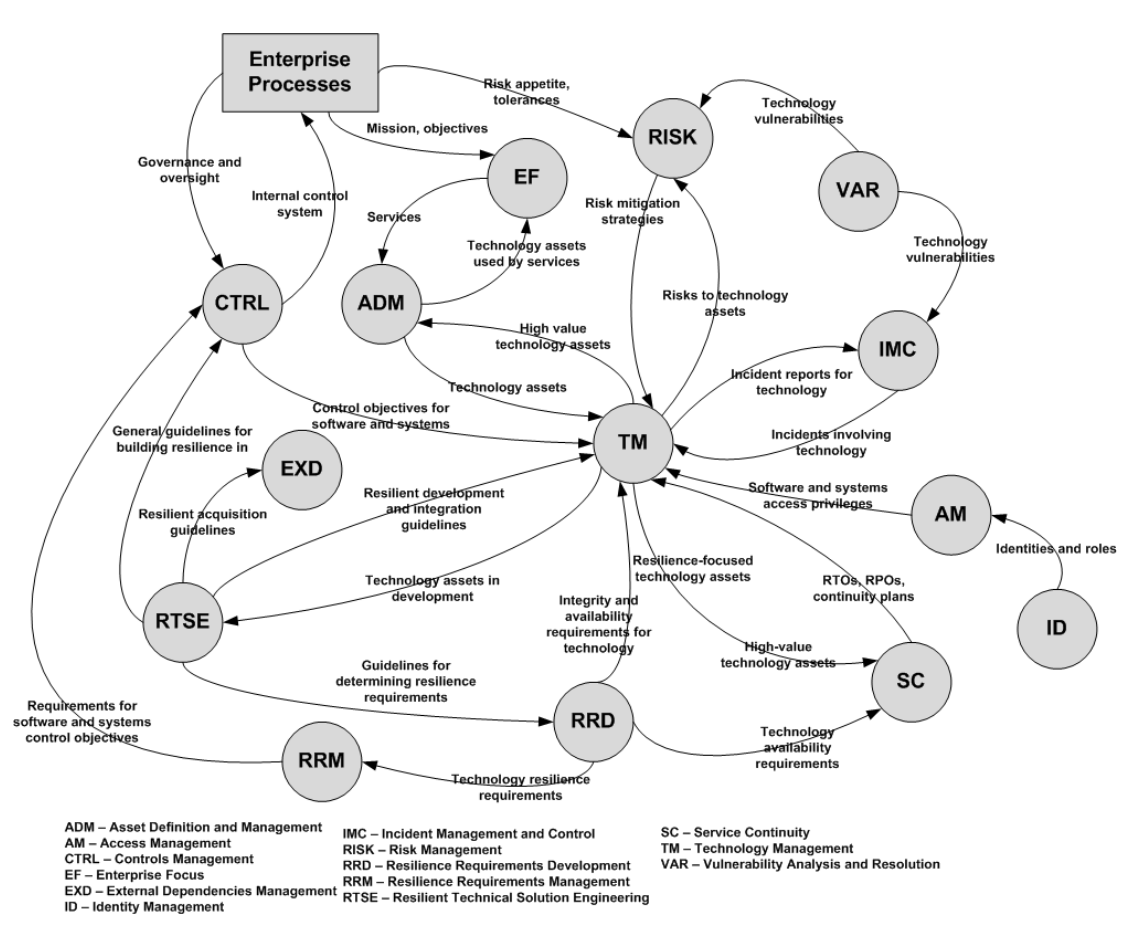


Figure 25: Relationships That Drive Technology Resilience

Facilities

Figure 26 shows the CERT-RMM process areas that drive the operational resilience management of facilities. As with information and technology assets, relationships that drive the resilience of facilities have special considerations, such as protecting facilities from disruption, ensuring that facilities are sustained, managing the environmental conditions of facilities, determining the dependencies of facilities on their geographical region, and planning for the retirement of a facility. Because facilities are often owned and managed by an external entity, consideration must also be given to how external entities implement and manage the resilience of facilities under the organization's direction.

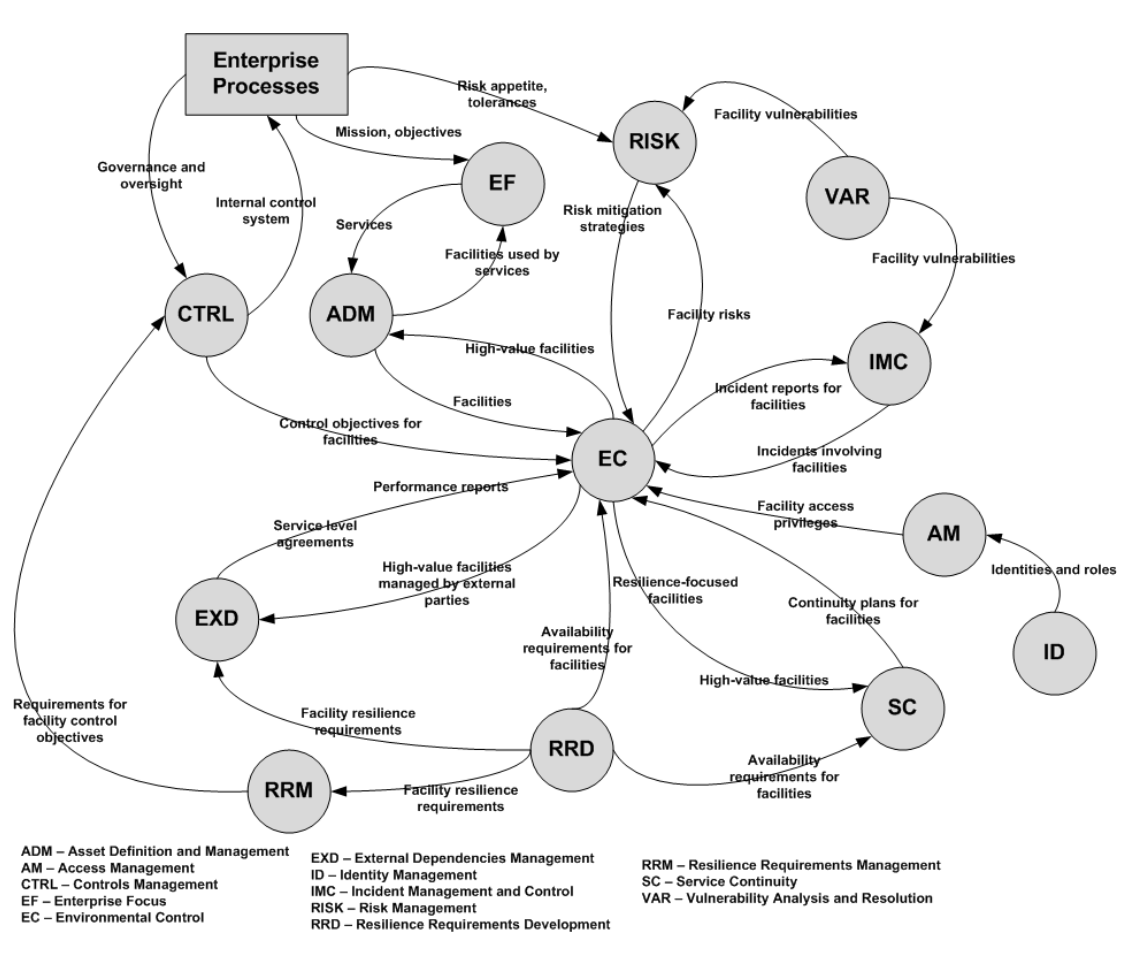


Figure 26: Relationships That Drive Facility Resilience

Part Two: Process Institutionalization and Improvement

The concept of using a capability model to improve operational resilience may not at first glance appear to provide significant advantages over the simple implementation of a code of practice. Codes of practice, after all, typically represent a cumulative view of how an industry faces a challenge such as information security and can be of great benefit to all organizations that share this challenge. For some organizations, using practices alone will bring about improvement—improvement in the way that passwords and user IDs are managed, how incidents are handled, or how continuity plans are developed and tested. But lasting improvement depends on the organization's ability to develop and inculcate a culture around managing operational resilience—that the operational resilience of the organization is everyone's job and responsibility. Security and continuity training and awareness alone do not create such a culture or provide it with the foundation it needs to flourish, particularly under times of stress.

At its core, a capability model is about improving the organization's capacity and competency for producing high-quality results, no matter the circumstances. Using such an approach, the practices performed by the organization are embedded within a culture of improvement so that the performance of these practices is measured and improved and the capability is sustained. This is critical in managing operational risk because not all risks can be identified, and responses to realized risk cannot always be planned.

A capability model provides a platform for measuring process institutionalization—the degree to which a process is embedded in the culture. Measuring the level of institutionalization of operational resilience management processes tells the organization something about how likely it is to retain these processes in changing risk environments.

In Part Two of this technical report, we discuss the capability dimension of CERT-RMM and the impact it can have on transforming the organization's performance. We also provide guidance on how to use the model to begin an improvement effort or to get a "health check" on how your organization is managing operational resilience today.

5 Institutionalizing Operational Resilience Management Processes

5.1 Overview

This section describes the process institutionalization aspects of CERT-RMM. It describes the "continuous representation" of CERT-RMM, the resultant capability levels, and the associated generic goals and generic practices of CERT-RMM, which have been sourced intact from CMMI. These model components directly address process institutionalization.

The "capability" dimension of CERT-RMM sets it apart from other models in the operational resilience space because this dimension determines the degree to which

- a process (or a practice) has been ingrained in the way work is defined, executed, and managed
- there is commitment and consistency to performing the process

Higher degrees of process institutionalization often equate to more stable processes that produce consistent results over time. Highly institutionalized operational resilience management processes should help the organization to improve service resilience not only because the process is stable but also because institutionalized processes are more likely to be retained during times of stress. Because the operational resilience of an organization is fundamentally tied to how well it performs during times of stress, the capability dimension of CERT-RMM is foundationally important to any organization that wants to improve its operational resilience.

5.2 Understanding Capability Levels

CERT-RMM is not a prescriptive model; that is, there is no guidance provided to adopt the model in any sequential or prescriptive path. Process improvement is unique to each organization, thus CERT-RMM provides the basic structure to allow organizations to chart their own specific improvement path using the model as the basis.

The ability to incrementally improve processes in an individual process area (or a group of process areas) is embedded in the model's *continuous representation*.[9] The improvement path in a continuous representation is defined by *capability levels*. Levels characterize improvement from an ill-defined state to a state where processes are characterized and used consistently across organizational units. This concept is an important enabler of the principle of convergence, particularly in large, distributed organizations.

[9] In CERT-RMM, there is no staged representation as in CMMI models. The staged representation uses *maturity levels*, which define levels of organizational maturity. In addition, the levels in a staged representation correlate to a collection of process areas that are prescribed or ~~-~~staged" at each level. This concept does not exist in CERT-RMM because all improvement activities are undertaken in an individual process area or a collection of process areas that are chosen by the organization to satisfy their unique process improvement objectives.

To reach a particular level, an organization must satisfy all of the appropriate goals of the process area (or a set of process areas) as well as the generic goals that apply to the specific capability level. The structure of the continuous representation for CERT-RMM is provided in Figure 27.

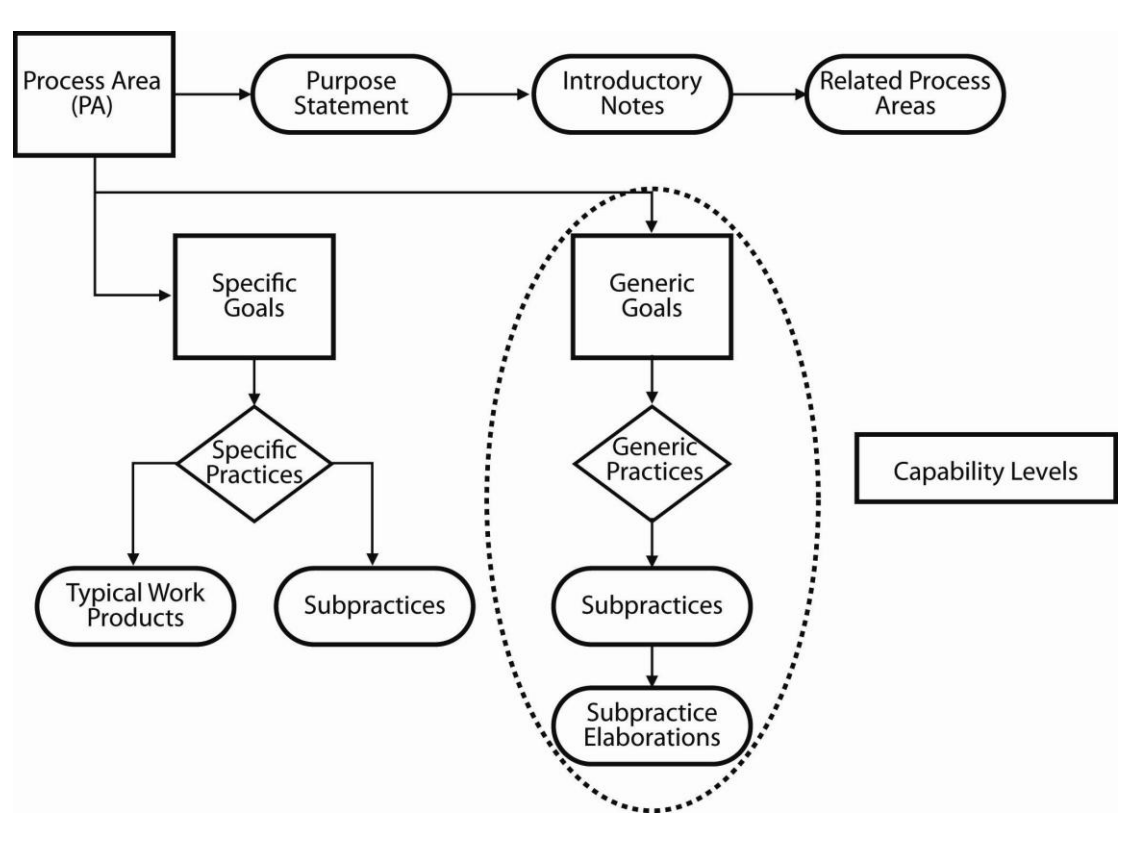


Figure 27: Structure of the CERT-RMM Continuous Representation

Because there is no staged representation in CERT-RMM, technically the concept of organizational maturity for managing operational resilience processes doesn't exist. However, it could be argued that an organization that reaches higher capability levels in each process area is exhibiting a higher degree of organizational maturity.

The capability dimension of CERT-RMM is also used for process improvement appraisal activities. Appraisal activities are described in Section 6.4.

CERT-RMM currently defines four capability levels, designated by the numbers 0 through 3, as follows:

Table 6: Capability Levels in CERT-RMM

Capability Level Number	Capability Level
0	Incomplete
1	Performed
2	Managed
3	Defined

A capability level for a process area is achieved when all of the generic goals are satisfied up to that level. By design, capability level 2 is defined by generic goal 2 and capability level 3 is defined by generic goal 3. Thus, the generic goals and practices at each level define the meaning of the capability levels. Because capability is cumulative, reaching capability level 3 means that the organization is also performing the goals and practices at capability levels 1 and 2. (See Section 5.4 for more information about generic goals and practices.)

5.3 Connecting Capability Levels to Process Institutionalization

Capability levels describe the degree to which a process has been institutionalized. Likewise, the degree to which a process is institutionalized is defined by the generic goals and practices. Table 7 links capability levels to the progression of processes and generic goals.

Table 7: Capability Levels Related to Goals and Process Progression

Capability Level Number	Generic Goal Number	Capability Level	Progression of Processes
0	N/A	Incomplete	No process or partially performed process
1	GG1	Performed	Performed process
2	GG2	Managed	Managed process
3	GG3	Defined	Defined process

The progression of capability levels and the degree of process institutionalization is characterized in the following descriptions.

5.3.1 Capability Level 0: Incomplete

An incomplete process is a process that either is not performed or is partially performed. One or more of the specific goals of the process area are not satisfied. No generic goals exist for this level since there is no reason to institutionalize a partially performed process [CMMI 2007].

5.3.2 Capability Level 1: Performed

Capability level 1 characterizes a *performed* process. A performed process is a process that satisfies *all* of the specific goals of the process area.[10] It supports and enables the work needed to perform operational resilience practices as defined by the specific goals.

Although achieving capability level 1 results in important improvements, those improvements can be lost over time if they are not institutionalized. The application of institutionalization through the generic goals at levels 2 and 3 helps to ensure that improvements are maintained [CMMI 2007].

When organizations perform a compliance review against a code of practice, they are in essence evaluating whether a process is performed. However, because operational resilience management processes are critically important during times of stress, simply verifying that a process is performed does not provide any indication or predictability about how the organization will

[10] In CERT-RMM as in CMMI models, all of the specific goals of a process area must be satisfied to state that the process is being performed or that the organization is performing the process at capability level 1.

perform in the future. In CERT-RMM, two additional and important levels of capability can be evaluated—managed and defined—which provide a better indicator of an organization's ability to predict performance.

5.3.3 Capability Level 2: Managed

A capability level 2 process is characterized as a *managed* process. Because capability levels are cumulative, a managed process is a *performed* process that has the basic infrastructure in place to support the process. At capability level 2, the process is

- planned and executed in accordance with policy
- employs skilled people who have adequate resources to produce controlled outputs
- involves relevant stakeholders
- monitored, controlled, and reviewed
- evaluated for adherence to the organization's process description

A critical distinction between a performed and a managed process is that a managed process is planned, and the performance of the process is managed against the plan. Corrective actions are taken when the actual results and performance deviate significantly from the plan. A managed process achieves the objectives of the plan and is institutionalized for consistent performance [CMMI 2007].

The process discipline reflected by capability level 2 helps to ensure that existing practices are retained during times of stress [CMMI 2007]. From an operational resilience management perspective, it is at capability level 2 where the organization can begin to answer some vital questions about its viability in a complex, risk-evolving environment, such as

- Are we able and committed to achieving consistent results from our processes today and tomorrow?
- Can we repeat our current successes consistently over time?
- Can we achieve the same results from our processes under times of stress and when we don't have access to our best employees and other resources?
- Can we obtain consistent results from our processes across organizational units and lines of business?

Organizations operating at capability level 2 should begin to know with some degree of certainty that they can achieve and sustain operational resilience goals regardless of changes in risk environments or when faced with new and emerging threats. Thus, instead of shifting its planning and practices for security and business continuity to address the next new and sensational threat, the organization stays on course and defines and refines its processes to address *whatever* risk comes its way. This indicates that the organization has invested in and nurtured its capabilities for sustaining these practices through sponsorship, ability and commitment, institutionalization, and measurement.

5.3.4 Capability Level 3: Defined

A capability level 3 process is characterized as a *defined* process. A defined process is a *managed* process (capability level 2) that is tailored from the organization's set of standard processes

according to the organization's tailoring guidelines. The process also contributes work products, measures, and other process improvement information as organizational process assets for use by all organizational units [CMMI 2007].

What does this ultimately mean to the organization? One of the principle challenges for effective operational resilience management is the ability to get all parts of the organization to coalesce around common goals and objectives. When different parts of the organization operate with different goals, assumptions, and practices, it is difficult if not impossible to ensure that the organization's collective goals and objectives can be reached. This is particularly true with cross-cutting concerns such as operational risk management. If the organization's risk assumptions are not reflected consistently in security, continuity, and IT operations activities, the organization's risk management process will be less than effective and perhaps significantly detrimental to overall operational resilience.

At capability level 3, alignment begins to occur because the standards, process descriptions, and procedures used for operational resilience management at the organizational unit level are tailored from the organization's standard set of operational resilience management processes. At capability level 2, each organizational unit may be improving the degree to which processes are institutionalized for that unit, but the organization is not necessarily reaping improvement benefits as a whole. At capability level 3, this begins to occur because there is more consistency across units, and improvements made by each organizational unit can be accessed and used by the organization through an organization-level improvement infrastructure.

Another critical distinction at capability level 3 is that processes are typically described more rigorously than at capability level 2. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. At capability level 3, processes are managed more proactively using an understanding of the interrelationships of the process activities and details [CMMI 2007].

5.3.5 Other Capability Levels

If your organization uses the CMMI models, you are likely to be familiar with two other capability levels—capability level 4, quantitatively managed, and capability level 5, optimized. Both these levels address the use of statistical and other quantitative techniques to control and improve processes. Beginning at capability level 4, process quality and performance is understood in statistical terms, and at capability level 5, common causes of process variation are understood and utilized for improving the range of process performance.

In CERT-RMM, it is unclear at this point whether these capability levels exist for operational resilience management, or more distinctly, whether they have meaning. In other words, should an organization strive for some level of quantitatively managed operational resilience processes, and if so, what benefits would this bring to the organization? Thus, these additional levels are not defined in the model.

5.4 CERT-RMM Generic Goals and Practices

Generic goals and practices are common to all process areas. They are the roadmap for helping the organization raise its performance of each process area to the next capability level. The degree of process institutionalization is embodied in the generic goals and practices and expressed in the

names of the generic goals, except for goal 1, "Achieve specific goals," which refers to the achievement of all of the specific goals and the performance of all of the specific practices of a process area.

The generic goals and practices used in CERT-RMM have been sourced from CMMI models. Thus, if you are a current user of CMMI models, you will be able to use the same process institutionalization features of CMMI in your CERT-RMM process improvement effort. However, there are a few differences, mostly in wording.

- Generic practice 2.1 in CMMI models is "Establish an Organizational Policy," while in CERT-RMM the corresponding practice is "Establish Process Governance." In CERT-RMM, policy is an artifact of effective governance, which is required for all processes to reach capability level 2.
- CMMI generic practice 2.3, "Provide Resources," is similar between the models, but CERT-RMM expands the definition of "resources" to include financial resources.
- Generic practice 2.6 in CMMI is "Manage Configurations," but in CERT-RMM it is retitled as "Manage Work Product Configurations" to avoid confusion with traditional configuration management activities as defined in IT operations.
- CERT-RMM includes subpractices in its articulation of generic goals and practices, which were eliminated in current versions of CMMI models.

Remember, only the generic goals for capability levels 1, 2, and 3 from CMMI are included in CERT-RMM. The CERT-RMM generic goals and practices are included in Appendix A.

5.4.1 CERT-RMM Elaborated Generic Goals and Practices

Since generic goals and practices apply to each process area, naturally there is variation in how each generic goal and practice affects the core subject matter of a process area. For example, generic practice 2.1, which calls for governance over the process, will differ widely depending on whether the process deals with incident management or organizational training and awareness. Thus, in each process area, the CERT-RMM model includes customized examples of the generic goals and practices. These customized examples are called elaborations, and thus each process area has a unique set of elaborated generic goals and practices associated with it.

In this technical report, the elaborated generic goals and practices are provided for the Asset Definition and Management process area, which is presented in its entirety in Part Three on page 78. The elaborated generic goals and practices for all other process areas can be found at www.cert.org/resilience.

5.5 Applying Generic Practices

Applying the generic practices in CERT-RMM is mostly straightforward, but can be confusing. It is easiest to start with a simple example.

When you are achieving the specific goals of the Asset Definition and Management process area, you are formally identifying, documenting, and managing the assets that the organization depends on to ensure that high-value services meet their missions. Consider generic practice GG2.GP2, "Establish and maintain the plan for performing the process." In this context, generic practice

GG2.GP2 reminds you that you need to *plan* the activities related to identifying, documenting, and managing assets throughout their life cycle. Thus, the application of this generic practice improves the institutionalization of the Asset Definition and Management process area by instilling a planning discipline.

In some cases, the application of a generic practice to the specific goals in a process area will seem recursive. For example, consider the application of generic practice GG2.GP2 to a process area that already includes a specific goal directed at planning. In the Incident Management and Control process area, planning for incident management is a major aspect of the process. The application of the generic practice GG2.GP2 in this case reminds you that you must *plan* the activities involved in creating the plan for managing incidents.

5.6 Process Areas That Support Generic Practices

While generic goals and generic practices are the model components that directly address process institutionalization, some process areas also address institutionalization by supporting the implementation of the generic practices. Thus, implementing the specific practices in some process areas may also help with the implementation of a generic practice.

Table 8 shows the relationship between CERT-RMM process areas and generic practices.

Table 8: CERT-RMM Generic Practices Supported by Process Areas

Generic Practice	Related Process Area	How the Process Area Helps to Implement the Generic Practice
GG2.GP1 **Establish process governance**	Enterprise Focus	Enterprise Focus addresses the governance aspect of managing operational resilience. Mastery of the Enterprise Focus process area can help to achieve GG2.GP1 in other process areas.
GG2.GP3 **Provide resources**	Human Resource Management Financial Resource Management	Human Resource Management ensures that resources have the proper skill sets and their performance is consistent over time. Financial Resource Management addresses the provision of other resources to the process, such as financial capital.
GG2.GP4 **Train people**	Organizational Training and Awareness	Organizational Training and Awareness ensures that resources are properly trained.

Generic Practice	Related Process Area	How the Process Area Helps to Implement the Generic Practice
GG2.GP8 **Monitor and control the process**	Monitoring Measurement and Analysis	Monitoring provides the structure and process for identifying and collecting relevant information for controlling processes. Measurement and analysis provides general guidance about measuring, analyzing, and recording information that can be used in establishing measures for monitoring actual performance of the process [CMMI 2007].
GG2.GP10 **Review status with higher level managers**	Enterprise Focus	As part of the governance process, Enterprise Focus requires oversight of the resilience process including identifying corrective actions.
GG3.GP1 **Establish a defined process**	Organizational Process Definition	Organizational Process Definition establishes the organizational process assets necessary to implement the generic practice [CMMI 2007].
GG3.GP2 **Collect improvement information**	Organizational Process Definition Organizational Process Focus	Organizational Process Definition establishes the organizational process assets. Organizational Process Focus addresses the incorporation of experiences into the organizational process assets [CMMI 2007].

6 Using CERT-RMM

There are many effective and appropriate ways for an organization to use CERT-RMM to guide, inform, or otherwise support improvements to its operational resilience management activities. For those familiar with process improvement, CERT-RMM can be used as the body of knowledge that supports model-based process improvement activities for operational resilience management processes. However, not all organizations embrace the terms "process improvement" and instead are simply looking for a way to evaluate their performance or organize their practices. All of these uses of CERT-RMM are legitimate.

In this chapter, we briefly explore the ways in which an organization could use CERT-RMM and provide a broader understanding of the concepts that are important for an organization to determine how best to make use of CERT-RMM to meet its unique needs. Section 6.1 provides selected examples of how the model can be effectively used by an organization. One such example is to use CERT-RMM to support model-based process improvement, a process which is more fully described in Section 6.2. Section 6.3 details a number of decisions around the scope of a CERT-RMM-based improvement effort, such as the organizational scope (which business units are involved), the model scope (which process areas are included), and the capability level targets (selecting "Performed," "Managed," or "Defined" as the target for each process area). Using the model as a basis for diagnosis can be accomplished in a variety of ways ranging from a formal appraisal to an informal review, as described in Section 6.4. Gaps that may be revealed through diagnostic methods should be analyzed in consideration of the improvement objectives to make sure that closing the gaps would be of value to the organization. Part of planning improvements to existing practices or planning the implementation of new practices is to determine where in the organization the practices will be performed or instantiated. Gap analysis and implementation planning are discussed in Section 6.5.

6.1 Examples of CERT-RMM Uses

This section provides several examples of how CERT-RMM can be used. This is not a complete list, but provides insight into how CERT-RMM can be applied to a broad set of challenges and objectives. The examples given describe using CERT-RMM to

- support the achievement of strategic and operational objectives
- evaluate, guide, and compare the implementation of resilience activities
- organize and structure the use of many codes of practice
- catalyze model-based process improvement

6.1.1 Supporting Strategic and Operational Objectives

CERT-RMM can be used as a source of guidance and information to support the achievement of specific objectives related to security, business continuity, IT operations, or managing operational risk in general. Organizational objectives that are directly or indirectly tied to resilience management activities can be strong drivers for CERT-RMM-based improvements.

Such objectives may be high-level and strategic. For example, consider an organization that sells various products both online and in its brick-and-mortar stores. The organization has established a strategic objective to increase the relative percentage of online sales by 25 percent over three years. Operational risk has been identified as a key constraint to the strategy—publicity associated with security breaches and downtime associated with business continuity failures could severely impede the achievement of the strategic objective. This organization can use CERT-RMM to guide the convergence and improvement of its security and business continuity processes to control and manage operational risks that could undermine achievement of this strategic objective.

Such objectives could also be more tactical. For example, consider an organization that recently suffered financial losses when information systems were offline following a security incident. Prior to the incident, warning signs were clear but had not been recognized. During the incident, confusion and ad hoc procedures resulted in longer downtime. The organization now understands that both its monitoring activities and its incident management activities need to be improved to avoid such losses in the future. CERT-RMM can be used to determine the degree of improvement necessary, guide these improvements, and measure the extent to which the improvements are institutionalized.

6.1.2 A Basis for Evaluation, Guidance, and Comparison

CERT-RMM is the codification of an extensive body of knowledge. It includes

- security practices and security management experience, from CERT and other reputable organizations and thought leaders, that have been developed based on years of work with public and private sector organizations on security improvement
- business continuity expertise from numerous financial industry organizations that were involved in the development of the model and for whom business continuity and disaster recovery requirements are critical to their organizational survival
- converged security, business continuity, and IT operations practices from numerous practice bodies and standards

Many professionals with responsibilities for their organization's operational resilience activities will find the model to be a useful basis to support the design, review, and comparison of such activities. Such guidance can be particularly useful when converging existing practices or when implementing new activities.

For example, consider an organization that has recently experienced an increase in access problems: employees with appropriate credentials have been unable to access certain systems and facilities. The team that has been assembled to diagnose the problem and propose improvements can use the Access Management (AM) and Identity Management (ID) process areas as reference sources for evaluating the current practices. If deficiencies are discovered, the model can be used as a source of guidance for improving practices or implementing new practices to address the issue.

Organizations and groups will also find the model to be a useful basis for characterizing, comparing, and learning from one another's practices. Diagnostic activities as described in Section 6.4.1 can be used as a basis for formal or informal comparisons among organizations of their respective implementation and institutionalization of resilience activities. Formal

benchmarking can be a valuable activity for industry groups to evaluate their collective resilience posture or for the components of a large enterprise to ensure that the overall enterprise is similarly prepared. Informal comparisons can also provide insights and support information sharing among a group of organizations.

6.1.3 An Organizing Structure for Deployed Practices

Many organizations have implemented practices from best practice bodies or standards related to security, business continuity, and IT operations. Sometimes, such organizations discover that these practices

- might not be providing the benefit that the organization expected
- may be performed less consistently than when first implemented
- might have eroded in their effectiveness because the organization has changed or the operational risk environment for the organization has changed

CERT-RMM can be used to guide the implementation of a process superstructure that will serve to refresh, institutionalize, integrate, streamline, and give purpose to the practices that have already been implemented. The concept of a "superstructure" is not meant to imply an additional layer of activities, though that might be appropriate in some organizations and in some circumstances. An effective and efficient process superstructure can be implemented by following the guidance in the model for converging the various operational risk management practices to ensure that they are based on common and consistent risk assumptions and that they are being performed to support organizational objectives.

The model can also be used to support the institutionalization of existing practices to ensure that they are reliably and consistently performed, especially in times of stress, and without a dependence on specific people or operating parameters that may not be present during a time of stress.

6.1.4 Model-Based Process Improvement

By far, organizations will find CERT-RMM most beneficial for process improvement. The unique aspects of CERT-RMM—the process focus and the capability dimension—were developed to help organizations evolve to a more enlightened treatment of managing operational resilience and sustaining capabilities over the long run. Regardless of the scope of improvement—a single aspect of operational resilience such as incident management or a comprehensive and broad view that incorporates all 26 process areas—CERT-RMM was built to enable an organization to easily begin a process improvement approach.

6.2 Focusing CERT-RMM on Model-Based Process Improvement

Most process improvement efforts can be structured to answer some variation of the following four questions:

- How do I decide what to do and in what order?
- How do I do it?
- How do I know if what I did worked?
- How do I decide what to do next?

These four questions can be directly mapped to the Plan, Do, Check, Act (PDCA) cycle, which was based on W. Edwards Deming's Shewhart cycle [Deming 2000, Imai 1986]. Effective methods for improvement and management of change typically use some variation of this approach. This section starts with identifying the impetus or stimulus for change and making the business case to initiate a process improvement program. It then describes an effective process for initiating any organizational change. Specific considerations for RMM-based process improvement are described in Section 6.3.

6.2.1 Making the Business Case

In today's business climate, organizations are constantly dealing with the demand to do more with less. The resources required to run the business, let alone to invest in new initiatives, are always at a premium—time, money, staff expertise, information, technology, and facilities, not to mention energy and attention span. All investment decisions are about doing what is best for the organization (and its stakeholders). However, what is best is sometimes hard to define, hard to quantify, and even harder to defend when the demand for investment dollars exceeds the supply.

Business leaders are increasingly aware of the need to invest in operational resilience—to better prepare for and recover from disruptive events, to protect and sustain high-value services and supporting assets (information, technology, facilities, and people) that are essential to meet business objectives, and to satisfy compliance requirements. So how do we ensure that investments in operational resilience will increase our confidence that services will continue to meet their mission, even during times of stress and disruption? And by so doing, how are we able to justify such investments to senior managers?

Making the business case for operational resilience, and specifically for investing in the adoption of CERT-RMM processes, is accomplished by articulating the business need and showing how CERT-RMM meets it—in a tangible and measurable way over a reasonable period of time for an affordable cost with a positive return. A well-articulated business need is the driver and stimulus for change. In the context of operational risk, it is often the answer to the question, Where does it hurt the most? or What high-impact, high-loss event(s) would put us out of business? A key step in this process is to identify the senior manager who most cares about the answer to these questions and to make sure he or she is on board as the visible champion and sponsor of the CERT-RMM improvement program.

In addition, those making the case for operational resilience must be able to demonstrate that investments are subject to the same decision criteria as other business investments, so that they can be prioritized, evaluated, and traded off in a similar fashion. Again, this ties back to business mission, strategic objectives, and critical success factors, which are the basis for determining the high-value services that support the accomplishment of strategic objectives (refer to the Enterprise Focus process area). Protecting and sustaining high-value services is the name of the game.

Once the business need is agreed to and a decision is made to take action to meet it, what is needed next is a process for ensuring that the need is met.

6.2.2 A Process Improvement *Process*

In large part, process improvement is about managing change, whether intentional or unintentional (including change caused by a disruptive event). The SEI has adapted Deming's

PDCA approach into a method for technology adoption and software process improvement called IDEAL[SM]. The IDEAL model is an organizational improvement model that serves as a roadmap for initiating, planning, and implementing improvement actions [McFeeley 1996]. The IDEAL model is named for the five phases it describes: initiating, diagnosing, establishing, acting, and learning, as shown in Figure 28.

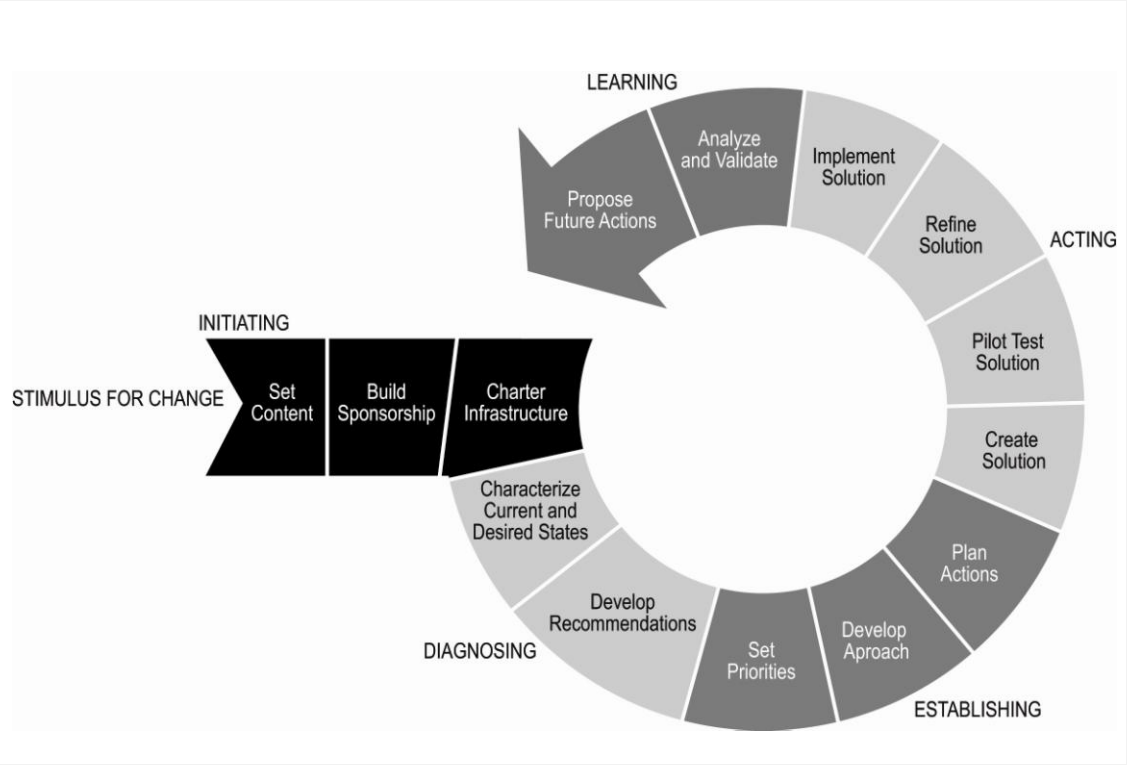


Figure 28: The IDEAL Model for Process Improvement

The catalyst that causes an organization to execute IDEAL is described above: identifying a business need, making the case for meeting it, and using it as the impetus or stimulus for change. This can include an objective to be met (such as those noted in Section 6.1.1), unanticipated events or circumstances, a new compliance requirement, or a problem to be solved, such as a poor organizational response to a disruptive event or a security breach.

Critical groundwork is completed during the initiating phase. The business reasons for undertaking the improvement effort are clearly articulated. The effort's contributions to business goals and objectives are identified. The support of managers that will serve as visible sponsors and champions for the effort is secured, and resources are allocated on an order-of-magnitude basis. Finally, an infrastructure for managing implementation details is put in place.

The diagnosing phase builds upon the initiating phase to develop a more complete understanding of the improvement effort. During the diagnosing phase, two characterizations of the organization are developed: the current state of the organization and the desired future state. These organizational states are used to develop an approach for improving business practice. The CERT-RMM capability appraisal is focused on the diagnosing phase of IDEAL. (See Section 6.4.1 for more details on the appraisal process.)

The purpose of the establishing phase is to develop a detailed work plan. Priorities are set that reflect the recommendations made during the diagnosing phase as well as the organization's broader operations and the constraints of its operating environment. Specific actions, milestones, deliverables, and responsibilities are incorporated into an action plan.

The activities of the acting phase help an organization implement the work that has been conceptualized and planned in the previous three phases. These activities will typically consume more calendar time and more resources than all of the other phases combined.

The learning phase completes the improvement cycle. One of the goals of the IDEAL model is to continuously improve the ability to implement change. In the learning phase, the entire IDEAL experience is reviewed to determine what was accomplished, whether the effort accomplished the intended goals, and how the organization can implement change more effectively and/or efficiently in the future. Records are kept throughout the IDEAL cycle with this phase in mind. These include CERT-RMM work products such as changes to resilience requirements, updates to service continuity plans, and incident reports.

As with any process improvement activity, some phases and activities such as those described for IDEAL are generic—they can be interpreted and applied with minimal customization based on the specific improvement initiative. Correspondingly, there are phases and activities that will require interpretation and tailoring when considering CERT-RMM in its entirety or when the focus of improvement is on specific process areas such as Incident Management and Control or Service Continuity. The remainder of this section describes some unique considerations or applications of the IDEAL model when using it as the basis for improving operational resilience management processes as defined in CERT-RMM.

6.3 Setting and Communicating Objectives Using CERT-RMM

A key element of any improvement effort is to establish and communicate clear improvement objectives. In addition to the stimulus for change or business objectives for change described in Section 6.1.1, objectives for a CERT-RMM-based improvement effort should include a clear delineation of scope. Scoping an improvement effort includes two key parts: the *organizational scope* and the *model scope*. The organizational scope is simply the part of the organization or an activity of the organization that is the focus of the improvement effort. Section 6.3.1 describes the elements and terminology of organizational scoping. The model scope is the designation of which parts of the CERT-RMM will be used to guide the improvement effort. Section 6.3.2 provides information on how to establish a model scope and describes both coarse-grained and fine-grained scoping options that are available in CERT-RMM.

Most improvement efforts will include capability level targets for selected CERT-RMM process areas. Establishing such targets is an effective and efficient way to communicate the extent of process institutionalization that is desired for the organization. Section 6.3.3 provides information on establishing and communicating capability level targets.

When scoping an improvement effort or establishing capability level targets for an improvement effort, it is important to consider the following.

- **organizational or strategic objectives**—Both the organizational scope and the model scope should be set in the context of the organizational or strategic objectives that are driving the

change. Some parts of the organization might be more or less appropriate for inclusion in the scope based on such objectives. The parts of the model that are included in the model scope should be closely aligned to the overall objectives. Remember that the organizational or strategic objectives can be diverse—they can be as simple as improving sales or as complex as preventing further data breaches or denials of service.

- **timing**—The scoping and objectives for an improvement effort may change over the course of time as a result of planned or unplanned changes to the organization or its operating environment. It may also be appropriate to establish a time-phased approach for both scope and objectives to ensure that the improvement effort is able to generate visible results quickly enough to be sustained (in other words, consider tackling low hanging fruit to generate some quick wins to build momentum and support).
- **regulatory mandates or industry initiatives**—Sometimes the driver for change comes from outside the organization in the form of a new regulatory mandate or industry initiative. In these cases, both the organizational scope and the model scope may be determined by the external driver. A phased approach that expands the organization and model scope over time may be appropriate to ensure that the approach for dealing with an external driver is consistent with and supports business objectives (versus being a compliance checklist exercise).
- **sponsorship**—Scoping should always be established with a careful consideration of sponsorship. The organizational scope should generally be aligned to the organizational reach or influence of the sponsor, and the model scope should generally be aligned to the responsibilities of the sponsor. It may also be appropriate to consider a phased approach to sponsorship in which successive layers of sponsorship are identified and secured as the scope of the effort increases over time.

For any improvement effort or CERT-RMM deployment, it may be appropriate or necessary to iterate the selection of organizational scope, model scope, and capability level targets in order to optimize them to the objectives and sponsorship for the improvement.

6.3.1 Organizational Scope

The organizational scope is the part of the organization that is the focus of the CERT-RMM deployment. In broad terms, the organizational scope should be bounded so that there are clear lines drawn for what is included in the improvement activities. This section presents some language and conventions that can be used to establish and describe the organizational scope.

The simplest scheme for organizational scoping is to focus on an explicit part of the organization. However, an organization may choose to bound the improvement effort around a specific system (such as the payroll system), a network, or a specific service, or according to another convention that is consistent with the improvement objectives. For example, an organization that had a data breach on a classified system might bound the improvement effort around that system. Thus, the effort would focus on the services provided by the system (which must meet their mission consistently) and the assets related to the system. The effort might also include the organizational units that have responsibility for managing the system and ensuring its resilience.

CERT-RMM has a strong enterprise undertone. This is because effective operational resilience management requires capabilities that often have enterprise-wide significance, such as risk management. However, the enterprise nature of CERT-RMM should not be interpreted to mean that it must be adopted or applied at an enterprise-level. On the contrary, CERT-RMM can be most effective when applied to a well-defined organizational scope and where enterprise influences can be measured.

The following terms can be used to describe the organizational scope and will be used in Section 6.5 to describe planning issues associated with CERT-RMM deployment.

- **organizational unit**: a distinct subset of an organization or enterprise. Typically, the organizational unit is a segment or layer of the organizational structure that may be clearly designated by drawing a box around part of the organization chart.
- **organizational subunit**: any sub-element of the organizational unit. An organizational subunit is fully contained within the organizational unit.
- **organizational superunit**: any part of the organization that is at a higher level than the organizational unit.

The organizational scope is established by clearly identifying one or more organizational units that will be the focus of the improvement.

Figure 29 shows the typical relationship between organizational unit, organizational subunit, and organizational superunit on a generic organizational chart. In this example, the organizational unit is defined as a specific segment of the organization as shown on the organizational chart with multiple subunits. In this example, organizational superunit can be used to refer to element 1 on the organization chart, as shown; organizational superunit can also be used to refer to the entire organization.

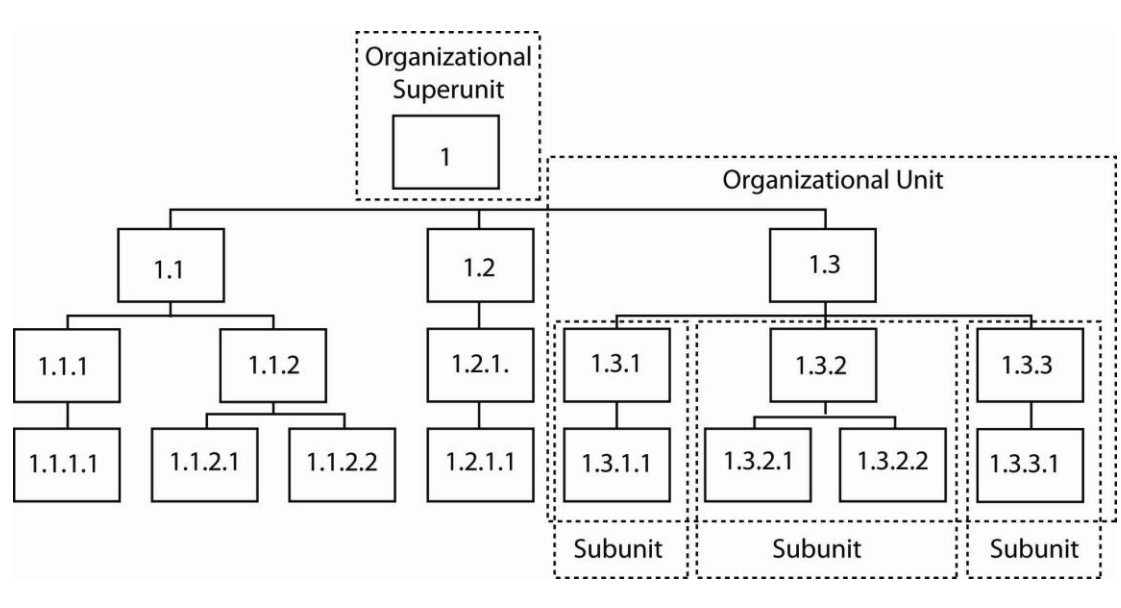


Figure 29: Organizational Unit, Subunit, and Superunit on an Organization Chart

For some improvement objectives, it may be optimal to designate an organizational unit that comprises all of the parts of the organization that are directly involved in the delivery of a specific service or that are responsible for a specific system. On an organization chart, such an organizational unit would be indicated by selecting the various elements of the organization that are responsible for the service, as shown in Figure 30. In this case, the term *organizational subunit* is less meaningful but could still be used to refer to elements such as 1.1.2 or 1.3.3.1. The term *organizational superunit* can be used to refer to element 1 or to the entire organization.

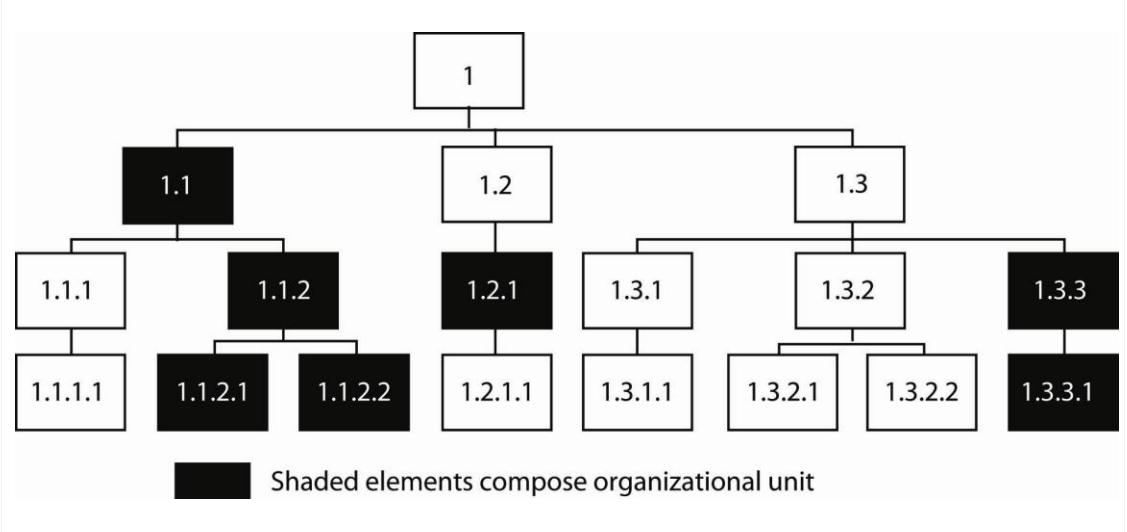


Figure 30: Alternate Organizational Unit Designation on Organizational Chart

6.3.2 Model Scope

The model scope represents the parts of CERT-RMM that will be used to guide the improvement effort. In other words, the model scope specifies which parts of the model will be deployed in the organizational units that compose the organizational scope.

The model scope is determined by selecting specific CERT-RMM process areas. Process areas should be chosen based on the objectives and business case for the improvement effort and in consideration of the other factors described above, such as timing, regulatory mandates, and sponsorship.

For example, the organization described in the first example in Section 6.1.1 might choose the following process areas as its initial model scope to help manage operational risk in support of its online sales growth objective:

- Service Continuity (SC)—to ensure that business continuity practices are adequate to sustain the operation of its online sales infrastructure
- Knowledge and Information Management (KIM)—to improve the protection of customer information
- Risk Management (RISK)—to establish common guidelines for risk tolerance and procedures to evaluate and mitigate identified risks in a consistent manner

- Communications (COMM)—to institute procedures and guidelines for communications that will support the organization's objective to preserve customer confidence even in times of stress

Similarly, the organization described in Section 6.1.1 as having suffered financial losses due to a security incident might choose the following process areas as its model scope to facilitate improvements to its incident management process and to implement more effective monitoring capabilities:

- Incident Management and Control (IMC)—to ensure that appropriate practices are institutionalized to support incident response
- Monitoring (MON)—to consistently instrument and monitor its operational environment so that potential threats can be identified early

Both example organizations might choose additional process areas in later phases of an improvement effort or might identify additional needs resulting from implementing improvements in these initial process areas.

There are no firm rules about the minimum or maximum number of process areas that should be selected to include in the model scope. Care should be taken to select as many process areas as needed to achieve the objectives, but few enough so that progress can be demonstrated in a reasonable time frame for the sponsor and key stakeholders. If the objectives require a large number of process areas, then a time-phased approach should be considered.

Targeted Improvement Roadmaps

Targeted improvement roadmap (TIR) is a term that is used to designate a specific collection of CERT-RMM process areas that serve a particular improvement objective. An organization could declare a TIR to represent its unique objectives for managing operational resilience, or might use a TIR that was designed by another organization or group. Industry groups might establish TIRs to represent their specific operational resilience concerns or to address an industry initiative or new regulatory mandate. Also, an organization could establish TIRs for specific tiers of suppliers or external dependencies, and use the TIRs to support the evaluation, selection, and monitoring of those entities. Appendix B contains several example TIRs.

In some cases, it may be appropriate to establish a finer-grained model scope than can be set by choosing entire process areas. CERT-RMM provides for several fine-grained scoping options that can be used in such cases, as described below.

Practice-Level Scope

Practice-level scope enables the model scope to be limited to selected specific and generic practices within a process area. This option does not have to be applied to all process areas when establishing the model scope, but may be appropriate for one or more process areas to address specific improvement needs or concerns. This scoping option may be useful in the early phases of an improvement effort, in response to very narrow improvement objectives, or to be consistent with the span of influence of the improvement sponsor.

For example, suppose that an organization's improvement objective is focused narrowly on information technology disaster recovery activities. From the Knowledge and Information

Management (KIM) process area, the organization might choose to include only specific practices KIM:SG5.SP3, Verify Validity of Information and KIM:SG6.SP1, Perform Information Duplication and Retention because it is concerned about its information backup practices and about ensuring the validity of information assets that will be used during disaster recovery operations.

Asset Scope

Because CERT-RMM addresses four asset types—people, information, technology, and facilities—the scope of the improvement effort could be focused on one or more process areas that could be tailored to focus on one or more asset types. For example, if the Asset Definition and Management process area is chosen, the scope of application of this process area could be limited to the "information" asset. Some process areas are already bound by an asset scope. These include Human Resource Management and People Management (people), Knowledge and Information Management (information), Technology Management (software, systems, and hardware), and Environmental Control (facilities). This option may be useful based on certain improvement objectives, a phased improvement strategy, or to tailor the model scope to best fit the span of influence of the improvement sponsor.

For example, an organization may limit the asset scope for phase 1 of a multiphased improvement project to information and technology assets only. This is consistent with the span of influence of the improvement sponsor and with the immediate organizational objective related to improving information security. If the model scope for the improvement project includes the Asset Definition and Management (ADM) process area, for phase 1 of the effort, ADM will be applied to information and technology assets only.

Resilience Scope

CERT-RMM addresses the convergence of three broad categories of operational resilience management activities: security, business continuity, and IT operations. Resilience scope is an option that limits one or more process areas to a subset of these resilience activities. This scoping option is useful in organizations where convergence of these activities is not yet occurring or where convergence is an organizational objective.

For example, an organization in which business continuity, security, and IT operations activities are still compartmentalized may initiate an improvement effort that is sponsored by the information security manager. The organization can use the resilience scope option to limit the interpretation of selected process areas so that they apply to security activities only. If the model scope includes the Compliance (COMP) process area, for example, it would be interpreted to apply exclusively to *security-related* compliance obligations.

Figure 31 shows the relationship of the four model scope options.

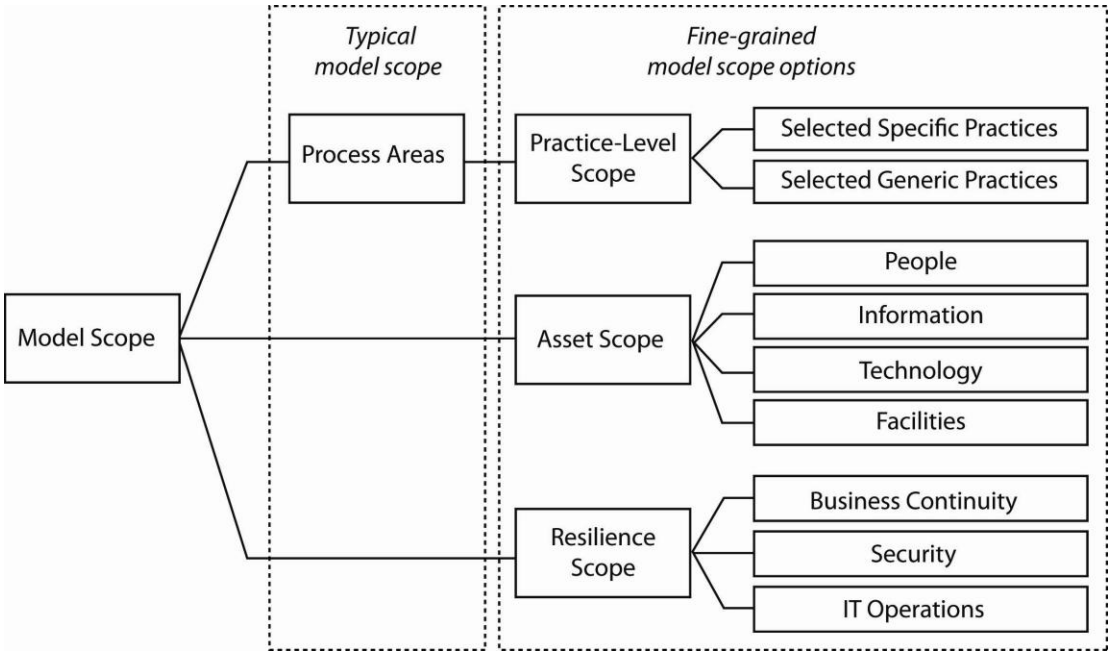


Figure 31: Model Scope Options

6.3.3 Capability Level Targets

Capability levels are used in the model to describe the achievement of the generic goals in a process area and are a measure of the extent to which a process area has been institutionalized (performed, managed, defined) by the organization (refer to Section 5.2). Establishing capability level targets is an important element in all CERT-RMM-based improvement efforts.

When establishing capability level targets, the organization should consider the importance of the generic practices relative to the organization's risk tolerance, threat environment, size, improvement timeframe, and improvement objectives. It may be valuable to review the generic goals and generic practices and envision what the implementation of those practices and the achievement of those goals would look like for the organization during normal operations and in times of stress. Capability level targets should be established for each process area and need not be the same. Capability level 1 (performed) may be completely appropriate for a process area, even if capability level 3 (defined) is the established target for another process area in the model scope. The capability level descriptions in Section 5.3 are valuable reference material for the selection of capability level targets.

Targeted Improvement Profile

Capability level targets can be efficiently communicated in a targeted improvement profile (TIP), which is typically represented as a bar chart showing the capability level target for each process area in the model scope. Figure 32 provides an example of a TIP for five process areas. Figure 33 provides another TIP example in which fine-grained scoping options have been selected for several of the process areas. A targeted improvement profile may be integrated with a targeted improvement roadmap. In this case, the TIR may include not only the process areas selected for a specific objective, but also the TIP, which describes the capability levels that must be achieved in each process area.

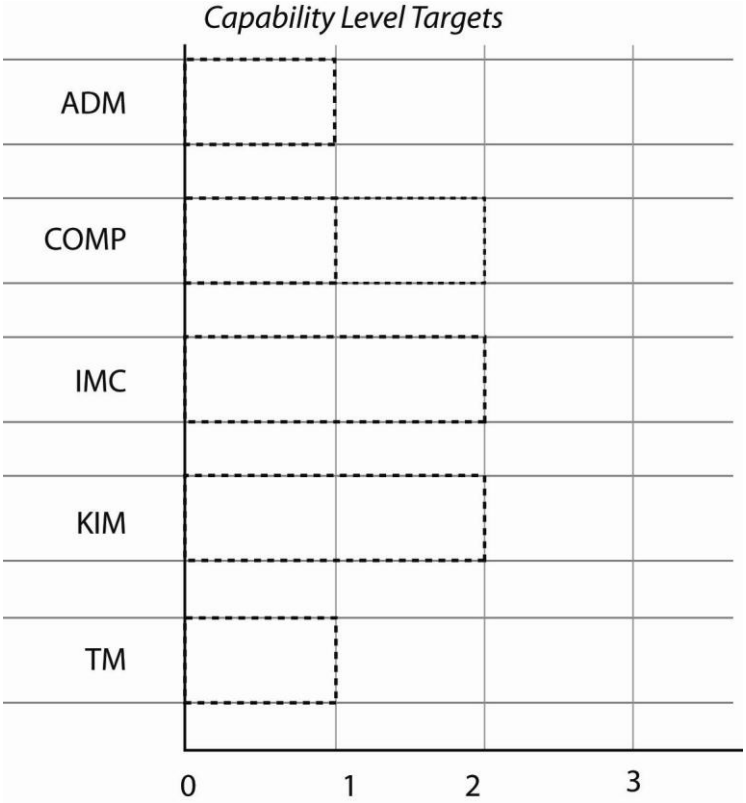


Figure 32: CERT-RMM Targeted Improvement Profile

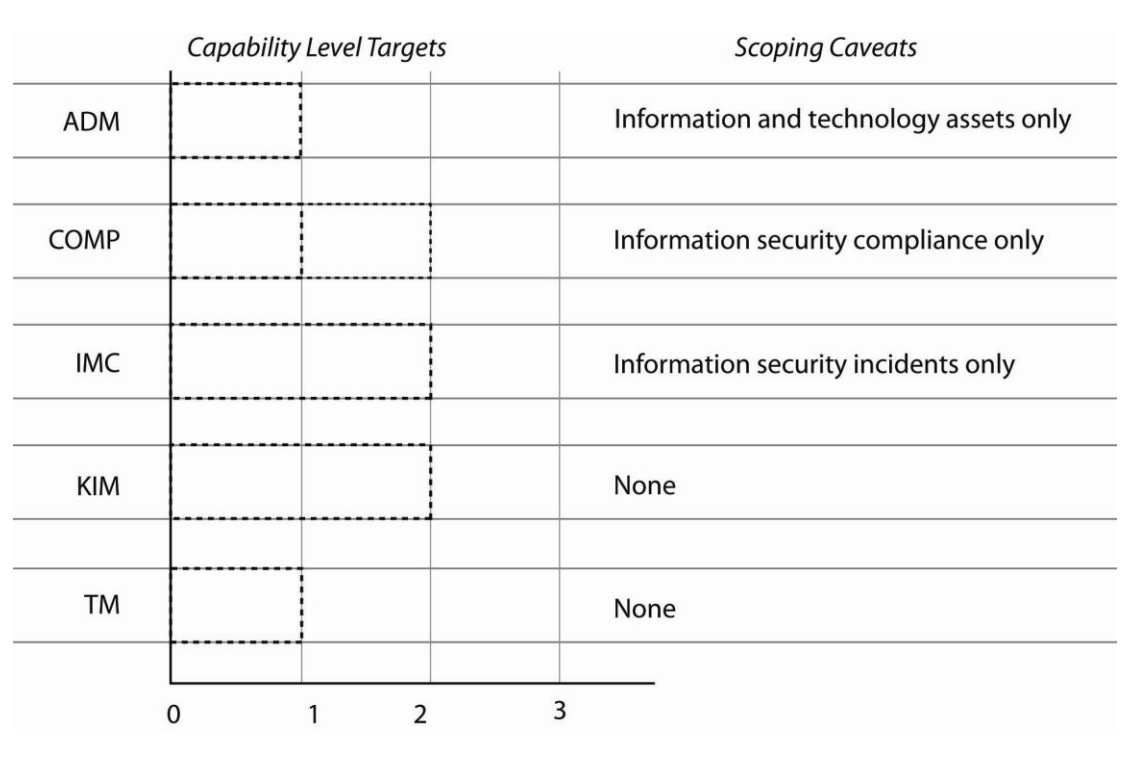


Figure 33: CERT-RMM Targeted Improvement Profile with Scope Caveats

The next section describes diagnostic methods that can be used to evaluate an organization to determine whether the capability level targets are being achieved.

6.4 Diagnosing Based on CERT-RMM

Diagnosing based on CERT-RMM is the process by which the model is used as a basis to evaluate the organization's current resilience practices. Diagnosing can be performed formally or informally, as described in the following sections.

6.4.1 Formal Diagnosis Using the CERT-RMM Capability Appraisal

Formal diagnosis based on CERT-RMM is performed using the CERT-RMM Capability Appraisal Method (CAM).[11] The CERT-RMM CAM is based on the Standard CMMI Appraisal Method for Process Improvement (SCAMPI), which has been used effectively by the CMMI community for many years [SCAMPI Upgrade Team 2006]. Similar to SCAMPI, three classes of CERT-RMM capability appraisals are available—A, B, and C—all of which are compliant with the Appraisal Requirements for CMMI (ARC) v1.2.

The class A appraisal is the most rigorous and the only one of the three methods that provides official capability level ratings. The class B appraisal has more tailoring options than class A and

[11] The CERT-RMM Capability Appraisal method definition document (MDD) is in development as of the publication of this report; once complete, the MDD will be available at www.cert.org/resiliency/rmm_appraisals.html.

results in the characterization of implemented practices in the organization according to a three-point scale. Class C is even more tailorable and can be used to evaluate planned approaches to practice implementation. Some distinctions among the three methods are provided in Table 9.[12]

Table 9: Classes of Formal CERT-RMM Capability Appraisals

Characteristic	Class A	Class B	Class C
Depth of investigation	High	Medium	Low
Objective evidence requirements	High	Medium	Low
Results provided	Capability level ratings and goal satisfaction ratings	Characterization of practice implementations on a three-point scale	Characterization of planned or intended practices on a flexible scale
Appraisal team size	4 or more	2 or more	1 or more
Allowed tailoring	Low	Medium	High
Resource requirements	High	Medium	Low

An organization might choose a class A appraisal because it desires a rigorous examination of implemented practices that produces a rating to acknowledge or memorialize its starting point or results for an improvement project. Class A appraisals are also useful when two or more organizations are to be compared, which might be of benefit in evaluating different parts of a large enterprise, for example.

At the other end of the spectrum, class C appraisals are fairly lightweight and can be flexibly used to evaluate planned implementations of practices or for a less rigorous examination of implemented practices. Large organizations might choose class C appraisals to evaluate the intent of organizational policies and guidelines relative to the model. This can be an effective and efficient way to evaluate whether the resilience policies and guidelines in a large enterprise would, if followed, produce the practices that are expected in the model.

Scoping an appraisal is an important activity in planning the appraisal. The same considerations for scoping an improvement project (as described in Section 6.3.1) are used in scoping an appraisal activity. The scope of an appraisal is typically the same as the scope of the improvement effort. However, it is not required that the scope of the appraisal or other diagnostic process match the scope of the overall improvement effort. In some cases, it may be efficient to diagnose at the operational subunit level.

Capability level ratings from class A appraisals can be shown as an overlay on the TIP diagram to clearly indicate gaps between the desired and current state as shown in Figure 34. Section 6.5 provides information about analyzing and using the gaps that are identified through diagnostic activities as input to planning improvements for an organization.

[12] For more on appraisal classes see http://www.sei.cmu.edu/cmmi/tools/appraisals/classes.cfm.

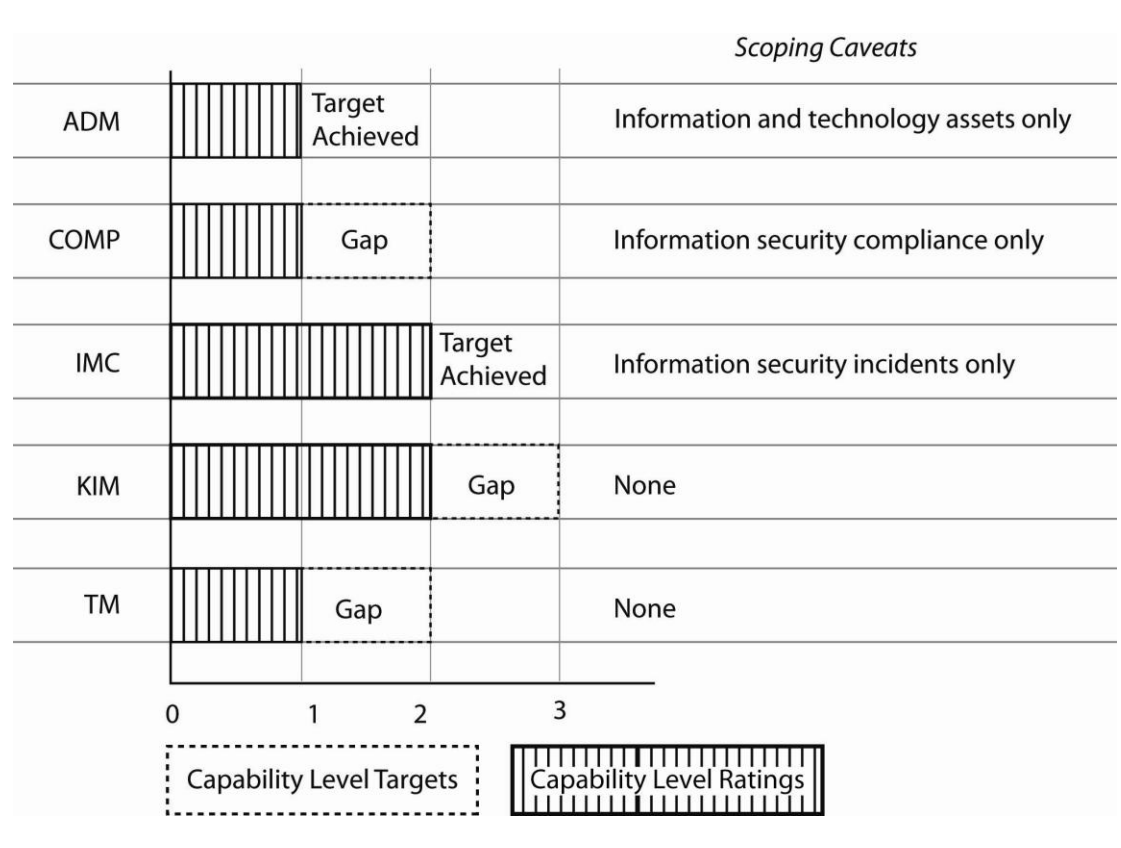


Figure 34: Capability Level Ratings Overlaid on Targeted Improvement Profile

Appraisal results can be an important diagnostic input to inform the starting point or results of an improvement effort. Informal diagnoses can also be useful, as described in the following section.

6.4.2 Informal Diagnosis

Informal diagnosis based on CERT-RMM includes any methods other than the formal appraisals described above that are used to compare the organization's practices to the guidance in CERT-RMM. Examples of informal diagnosis methods include

- meetings or tabletop exercises in which the people who are responsible for the practices in a given process area come together, review the model guidance, and discuss the extent to which the organization's practices achieve the model intent
- reviews or analyses performed by a single person or a small group to compare the organization's practices to the model guidance supported by written reports
- informal collection and review of evidence that demonstrates whether the organization is performing the model practices

In all cases, the outcomes of such diagnoses are informal findings related to the organization's performance as compared to the model guidance. Such activities can be useful to guide informal process improvement activities or to provide information for scoping or setting capability level targets for a more formal process improvement project. Informal reviews can also be useful when the model is being used as a basis for evaluation as described in Section 6.1.2.

Both formal and informal diagnostic activities provide valuable input for planning an improvement activity. Additional considerations for planning improvement activities are described in the next section.

6.5 Planning CERT-RMM-Based Improvements

When planning a CERT-RMM deployment, analyzing gaps and determining where various practices should be optimally implemented in the organization are key activities. CERT-RMM-specific considerations related to those activities are addressed in this section.

6.5.1 Analyzing Gaps

Diagnostic activities typically reveal gaps between current and desired performance. Such gaps are necessary input to planning improvements for an organization. However, before plans are established to close any gaps that are revealed, it is important to reconsider the identified gaps in light of the overall improvement objectives. The following questions may be useful in analyzing and prioritizing the gaps in support of the improvement planning process.

- Will closing a gap support the improvement objective?
- Is the cost of closing a gap justifiable in light of the improvement objective?
- Which of the identified gaps are most important to close first?
- Can the gap be closed in one improvement iteration, or should a phased approach be deployed?

If it is determined that one or more of the identified gaps are acceptable and will not be closed, it may be appropriate to revisit and revise the objectives for the improvement activity. This iterative approach is valuable to ensure that the organization is spending improvement resources in the most productive manner. For example, if the organization chose to focus improvement efforts on a recent data breach, analyzing gaps can help the organization to prioritize improvement activities to maximize outcome at the lowest cost.

6.5.2 Planning Practice Instantiation

Part of planning improvements to existing practices or planning the implementation of new practices is to determine where in the organization the practices will be performed or instantiated. The terms *organizational unit*, *superunit*, and *subunit* (see Section 6.3.1) can be valuable in describing where a particular practice is to be performed in relation to the organizational scope for the improvement campaign.

Most organizations will find that different practices within a single CERT-RMM process area may be optimally performed at different levels in the organization. For example, in the Service Continuity (SC) process area, a large organization might choose to implement specific practice SC:SG1.SP2, Establish Standards and Guidelines for Service Continuity, at a very high level in the organization so that a consistent set of standards and guidelines are established and deployed across the organization. The same organization might choose to implement specific practice SC:SG3.SP2, Develop and Document Service Continuity Plans, at a much lower level in the organization.

If the immediate or long-term improvement objective for a given process area is to achieve capability level 3, planning should include the determination of where the organizational process assets will reside. (This can be done using OPD:SG1.SP3, Establish the Organization's Measurement Repository, and GG3, Institutionalize a Defined Process.) If the long-term plan includes a larger organizational scope than the immediate plan, then the optimal location for the organizational process assets might be different than would be indicated by the immediate plan. Strategic consideration should be given to this issue to avoid unnecessary rework in future improvement phases. For example, Figure 35 shows two alternative locations for the organizational process assets in an organization. If the organization never plans to deploy CERT-RMM beyond the organizational unit shown in the figure, then either location for the organizational process assets will suffice. Suppose however, that the organization ultimately plans to deploy CERT-RMM to the units designated by 1.1 and 1.2; in this case, the organizational process assets should be located at the highest level in the organization.

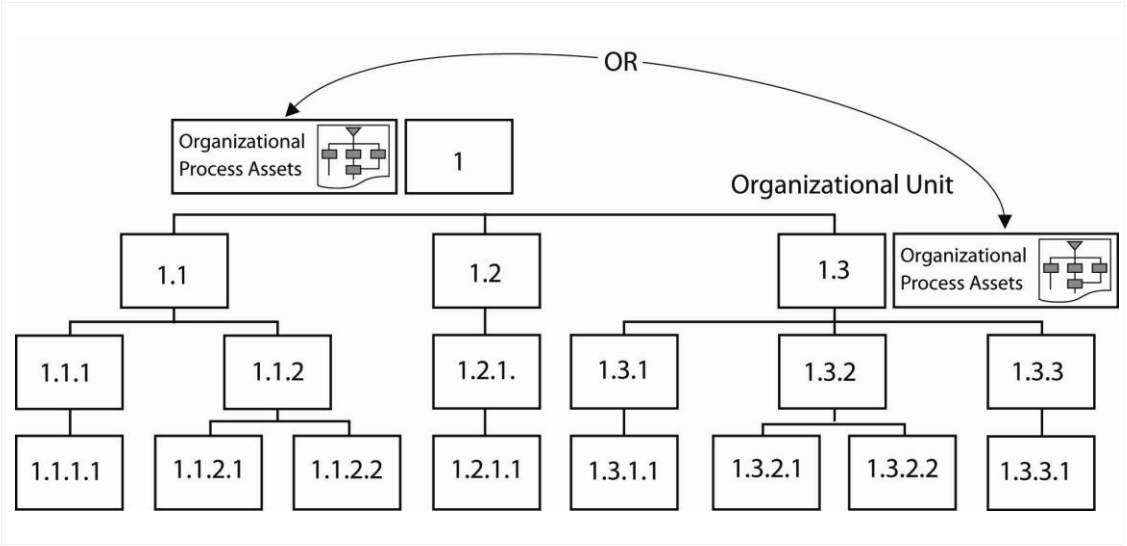


Figure 35: Alternate Locations for Organizational Process Assets

CERT-RMM is agile and flexible enough to support a wide range of improvement activities in an organization. The key to any successful improvement effort is to understand the objectives and to design the improvement activity to accomplish those objectives. Fine-grained scoping options are available in CERT-RMM to enable an organization to optimize the organization and model scope for an improvement. Formal and informal methods for diagnosis and comparison are available to use the model as a basis for evaluation and gap identification.

Part Three: CERT-RMM Process Areas

In Part Three, we present the CERT-RMM process areas. To limit the length of this technical report, the process areas are presented in outline form (with one exception as noted below). For each process area, the outline form includes full versions of the purpose statement, introductory notes, related process areas, and the summary of specific goals and practices. At the specific goals and practices level, only the goal and practice names and the goal and practice statements are provided. The remainder of informative material, including explanations, notes, elaborations, subpractices, and typical work products, are available for download by process area at www.cert.org/resilience.

In addition, the elaborated generic goals and practices for each process area are excluded from this document. Process areas posted on the website include elaborated generic goals and practices that can be used to help you improve performance.

In Part Three, the Asset Definition and Management process area is provided in its entirety as an example. This will give you a sense of what is contained in a process area and the level of detail you can expect if you download the additional process areas from the website. This process area includes elaborated generic goals and practices.

To facilitate the evolution and calibration of the model, the CERT website will always contain the most current versions of the process areas, as well as new process areas. Please visit this space often to obtain the most up-to-date information about the model.

ASSET DEFINITION AND MANAGEMENT

Engineering

Purpose

The purpose of Asset Definition and Management is to identify, document, and manage organizational assets during their life cycle to ensure sustained productivity to support organizational services.

Introductory Notes

Mission success for an organization relies on the success of each service in achieving its mission. In turn, mission assurance for services depends on the availability, productivity, and ultimately the resilience of high-value assets that the service relies upon—people to perform and monitor the service, information to fuel the service, technology to support the automation of the service, and facilities in which to operate the service. Whenever any high-value asset is affected by disruptive events (by the realization of operational risk), the assurance of the mission is less certain and predictable. An organization must be able to identify its high-value assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to services.

The Asset Definition and Management process area seeks to establish organizational assets as the focus of the operational resilience management process. High-value organizational assets are identified and profiled (establishing ownership, a common definition, and value), and the relationship between the assets and the organizational services they support is established. The organization also defines and manages the process for keeping the asset inventory current and ensures that changes to the inventory do not result in gaps in strategies for protecting and sustaining assets.

The Asset Definition and Management process area is a higher order competency that establishes the inventory of high-value organizational assets of all types. The resilience aspects of these assets (and their related services) are addressed in asset-specific process areas as noted in “Related Process Areas” below.

The Asset Definition and Management process area has three specific goals: to inventory assets, associate the assets with services, and manage the assets. To meet these goals, the organization must engage in the following practices:

- Establish a means to identify and document assets.
- Establish ownership and custodianship for the assets.
- Link assets to the services they support.
- Establish resilience requirements (including those for protecting and sustaining) for assets and associated services. (This is addressed in the Resilience Requirements Definition and Resilience Requirements Management process areas.)
- Provide change management processes for assets as they change and as the inventory of assets changes.

- Establish risk management processes to identify, analyze, and mitigate risks to high-value assets. (This is addressed in the Risk Management process area.)
- Establish continuity processes to develop, test, and implement service continuity and restoration plans for high-value assets. (This is addressed in the Service Continuity process area.)
- Monitor the extent to which high-value assets are adequately protected and sustained, and develop and implement adjustments as necessary. (This is addressed in the Monitoring process area.)

Related Process Areas

The identification, documentation, analysis, and management of asset-level resilience requirements are addressed in the Resilience Requirements Development and Resilience Requirements Management process areas.

The identification, assessment, and mitigation of risks to high-value assets is addressed in the Risk Management process area.

The development, implementation, and management of strategies for protecting people is addressed in the People Management process area.

The development, implementation, and management of strategies for protecting information assets is addressed in the Knowledge and Information Management process area.

The development, implementation, and management of strategies for protecting technology assets is addressed in the Technology Management process area.

The development, implementation, and management of strategies for protecting facility assets is addressed in the Environmental Control process area.

The development and implementation of service continuity plans for high-value assets and their related services is performed in the Service Continuity process area. Service continuity plans describe strategies for sustaining high-value assets and services.

The identification and prioritization of high-value organizational services is performed in the Enterprise Focus process area.

Summary of Specific Goals and Practices

Goals	Practices
ADM:SG1 Establish Organizational Assets	ADM:SG1.SP1 Inventory Assets
	ADM:SG1.SP2 Establish a Common Understanding
	ADM:SG1.SP3 Establish Ownership and Custodianship
ADM:SG2 Establish Relationship Between Assets and Services	ADM:SG2.SP1 Associate Assets with Services
	ADM:SG2.SP2 Analyze Asset-Service Dependencies
ADM:SG3 Manage Assets	ADM:SG3.SP1 Identify Change Criteria
	ADM:SG3.SP2 Maintain Changes to Assets and Inventory

ADM:SG1 Establish Organizational Assets

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

The assets of the organization must be identified, prioritized, documented, and inventoried.

The highest level concept in the operational resilience management process is a service. Services are defined as the limited number of activities that the organization carries out in the performance of a duty or in the production of a product. Services are the prime resource that the organization uses to accomplish its mission. Each service has a mission that must be accomplished in order to support the organization's strategic objectives. Failure to accomplish the mission of a service is a potentially serious impediment to accomplishing the organization's mission.

An important aspect of services is that they are "fueled" by assets—the raw materials that services need to operate.

A service cannot accomplish its mission unless there are

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

These assets may or may not be directly owned by the organization. For example, outsourcing of call center functions may mean that the organization does not control the people, information, technology, or facilities that enable the service; however, the organization retains responsibility for the ownership and resilience of the assets. In order to properly determine resilience requirements (and to implement appropriate strategies for protecting and sustaining assets), the organization must define these assets from a service perspective and establish ownership and responsibility for their resilience.

ADM:SG1.SP1 Inventory Assets

Organizational assets are identified and inventoried.

Success at achieving the organization's mission relies upon critical dependencies between organizational goals and objectives, services, and associated high-value assets. Lack of performance of these assets (due to disruptive events, realized risk, or other issues) impedes mission assurance of associated services and can translate into failure to achieve organizational goals and objectives. Thus, ensuring the operational resilience of high-value assets is paramount to organizational success.

The first step in establishing the operational resilience of assets is to identify and define the assets. Because assets derive their value and importance through their association with services, the organization must first identify and establish which services are of high-value. This provides

structure and guidance for developing an inventory of high-value assets for which resilience requirements need to be established and satisfied. Inventorying these assets is also essential to ensuring that changes are made in resilience requirements as operational and environmental changes occur.

Establishing criteria for determining the value of services and associated assets is performed in the Risk Management process area. Identifying and prioritizing high-value organizational services is performed in the Enterprise Focus process area.

Each type of asset for a specific service must be identified and inventoried. The following are descriptions of the four asset types.

People are those who are vital to the expected operation and performance of the service. They execute the process and monitor it to ensure that it is achieving its mission, and make corrections to the process when necessary to bring it back on track. People may be internal or external to the organization.

Information is any information or data, on any media including paper or electronic form, that is vital to the intended operation of the service. Information may also be the output or byproduct of the execution of a service. Information can be as small as a bit or byte, a record or a file, or as large as a database. (The organization must determine how granular to define information with respect to its purpose in a service). Because of confidentiality and privacy concerns, information must also be categorized as to its organizational sensitivity. Categorization provides another level of important description to an information asset that may affect strategies to protect and sustain it. Examples of information include social security numbers, a vendor database, intellectual property, and institutional knowledge.

Technology describes any technology component or asset that supports or automates a service and facilitates its ability to accomplish its mission. Technology has many layers, some which are specific to a service (such as an application system) and others which are shared by the organization (such as the enterprise-wide network infrastructure) to support more than one service. Organizations must describe technology assets in terms that facilitate development and satisfaction of resilience requirements. In some organizations, this may be at the application system level; in others, it might be more granular, such as at the server or personal computer level. Examples of technology assets include software, hardware, and firmware, including physical interconnections between these assets such as cabling.

Facilities are any physical plant assets that the organization relies upon to execute a service. Facilities are the places where services are executed and can be owned and controlled by the organization or by external business partners. Facilities are also often shared such that more than one service is executed in and dependent upon them. (For example, a headquarters office building has a substantial number of services being executed inside of it.) Facilities provide the physical space for the actions of people, the use and storage of information, and the operations of technology components. Thus, resilience planning for facilities must integrate tightly with planning for the other assets. Examples of facilities include office buildings, data centers, and other real estate where services are performed.

Organizations may use many practical methods to inventory these assets. Human resources databases identify and describe the roles of vital staff. Fixed asset catalogs often describe all levels of technology components. Facilities and real estate databases have information about high-value physical plant assets. However, bear in mind that internal databases may not cover people, technology, and facilities that are not under the direct control of the organization. In contrast to people, technology, and facilities, less tangible assets such as information and intellectual property may not be identified and regularly inventoried because they are often difficult to describe and bound. For example, a staff member may have information that is critical to the effective operation of a service that has not been documented or is not known to other staff members. This must be resolved in order to properly define security and continuity requirements for these assets.

Typical work products

1. Asset inventory (of all high-value assets of each type)
2. Asset database

Subpractices

1. Identify and inventory vital staff.
2. Identify and inventory high-value information assets.
3. Identify and inventory high-value technology components.
4. Identify and inventory high-value facilities.
5. Develop and maintain an asset database that establishes a common source for all high-value assets.

ADM:SG1.SP2 Establish a Common Understanding

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

Proper description of organizational assets is essential to ensuring a common understanding of these assets between owners and custodians. (The difference between owners and custodians is explained in ADM:SG1.SP3.) A consistent description aids in developing resilience requirements and ensuring satisfaction of these requirements. It defines the boundaries and extent of the asset, which is useful for defining ownership

and responsibility for the resilience of the asset. In addition, an asset's description can be easily communicated within and outside of the organization to facilitate communication of resilience requirements to internal constituencies and external business partners.

At a minimum, all high-value assets (as identified in ADM:SG1.SP1) should be defined to the extent possible. Differences in the level of description are expected from asset to asset, and an organization must decide how much information is useful in facilitating requirements definition and satisfaction. The description of the asset should detail why it is considered to be of high value to the organization. There are some common elements that should be collected, at a minimum, for each asset.

These are examples of information that should be collected and documented for assets:

- asset type (people, information, technology, or facilities)
- categorization of asset by sensitivity (generally for information assets only)
- asset location (typically where the custodian is managing the asset)
- asset owners and custodians (particularly where this is external to the organization)
- the format or form of the asset (particularly for information assets that might exist on paper and electronically)
- location where backups or duplicates of this asset exist (particularly for information assets)
- the services that are dependent on the asset *(see ADM:SG2)*
- the value of the asset in either qualitative or quantitative terms

An organization may also choose to document the asset's resilience requirements as part of the asset profile so that there is a common source for communicating and updating these requirements and so that their association with an asset is established. In addition, strategies to protect and sustain an asset may be documented as part of the asset profile. *(Resilience requirements for assets are developed and documented in the Resilience Requirements Development process area.)*

There are additional considerations for describing each type of asset.

People

In describing people, be sure to describe a role where possible, rather than the actual persons who perform the role. If a particular person or persons in the organization are vital to the successful operation of a service because of their detailed knowledge and experience, this should be noted in the description of the asset. This may affect the resilience requirements of the asset when defined.

Information Assets

Because information is an intangible asset, it must be accurately described. Some organizations find media conventions such as record, file, and database to be natural limiters of the description of an information asset. Information asset descriptions should also address the level of sensitivity of the asset based on the organization's categorization scheme. This will aid in ensuring that confidentiality and privacy sensitivities are considered in the development and satisfaction of resilience requirements.

Technology and Facilities Assets

Organizations often view technology components and facilities as shared enterprise assets. This should be considered when defining these assets and when developing resilience requirements. In addition, because technology and facilities are tangible assets, the current value of the asset should be included in the definition. This will provide additional data on the value of the asset to the organization and serve as a guide for comparing value versus cost of activities to protect and sustain assets.

Typical work products

1. Asset profiles (for all high-value assets of each type)
2. Updated asset database (including asset profiles)

Subpractices

1. Create an asset profile for each high-value asset (or similar work product) and document a common description.

   Be sure to address the entire range of information that should be collected for each type of asset, including at a minimum the owner and the custodian(s) of the asset. Also, include the resilience requirements of the asset as established or acquired by the organization. *Refer to the Resilience Requirements Development process area for more information.*

2. Describe and document the "acceptable use" of the asset. Ensure alignment between acceptable uses and resilience requirements.
3. Categorize information assets as to their level of sensitivity.
4. Update the asset database with asset profile information.

   All information relevant to the asset (collected from the asset profile) should be contained with the asset in its entry in the asset database.

ADM:SG1.SP3 Establish Ownership and Custodianship

The ownership and custodianship of assets is established.

High-value assets have owners and custodians. Asset owners are the persons or organizational units, internal or external to the organization, who have primary responsibility for the viability, productivity, and resilience of the asset. For example, an information asset such as customer data may be owned by the "customer relations department" or the "customer relationship manager." It is the owner's responsibility to ensure that the appropriate level of confidentiality, integrity, and availability requirements

are defined and satisfied to keep the asset productive and viable for use in services.

Asset custodians are persons or organizational units, internal or external to the organization, who are responsible for implementing and managing controls to satisfy the resilience requirements of high-value assets while they are in their care. For example, the customer data in the above example may be stored on a server which is maintained by the IT department. In essence, the IT department takes custodial control of the customer data asset when the asset is in its domain. The IT department must commit to taking actions commensurate with satisfying the owner's requirements to protect and sustain the asset. However, in all cases, owners are responsible for ensuring that their assets are properly protected and sustained, regardless of the actions (or inactions) of custodians.

In practice, custodianship brings many challenges for asset owners in ensuring that the resilience requirements of their assets are being satisfied. In some cases, custodians of assets must resolve conflicting requirements obtained from more than one asset owner. This can occur in cases where a server contains more than one information asset from different owners with unique and sometimes competing requirements. In addition, custodianship may occur outside of organizational boundaries, as is commonly seen in outsourcing arrangements. In such a case, asset owners must clearly communicate the resilience requirements of their assets to external custodians and must expend additional effort in monitoring the satisfaction of those requirements.

The owner of each high-value asset is established in order to define responsibility and accountability for the asset's resilience and its contributions to services. Accordingly, owners are responsible for developing and validating the resilience requirements for high-value assets that they own. They are also responsible for the implementation of proper controls to meet resilience requirements, even if they assign this responsibility to a custodian of the asset.

The identification, documentation, analysis, and management of asset-level resilience requirements are addressed in the Resilience Requirements Development and Resilience Requirements Management process areas.

Ownership of assets typically varies depending on the asset type.

- People are part of the organizational unit or line of business where their job responsibilities and accountabilities are managed. This organizational unit or line of business is considered the "owner" of these resources in that they have authority and accountability for their work assignments and their training, deployment, and performance.
- Information assets are generally owned by a person, organizational unit, or line of business where the asset originates (i.e., where the service is owned which the asset supports) or where responsibility for the asset's confidentiality, integrity, and availability has been established.
- Technology and facilities assets tend to be shared by the enterprise, and therefore it may be difficult to establish a single owner.
- Technology assets are most often owned by IT but could be owned by an organizational unit or line of business that manages their technology support structure separate from IT or the enterprise.
- Facilities may be owned by a central group (such as Facilities Management) or may be owned by an organizational unit or line of business.

In some cases, the organization may group a set of assets together into a service and identify an owner of the service. This aggregation often is more practical when there are many assets in an organization and strategies to protect and sustain at the asset level would not be practical.

The organization should also, to the extent possible, identify relevant custodians for each high-value asset. Custodians take custodial care of assets under the direction of owners and are usually responsible for satisfying the asset's resilience requirements on an operational basis. Identifying the custodians of high-value assets also helps to identify the operational environment of the assets where risks may emerge and where continuity plans would need to be implemented.

Typical work products

1. Owner identification
2. Custodial identification
3. Updated asset profiles (including owner and custodian)
4. Updated asset database (including owner and custodian)

Subpractices

1. Document and describe the owner of each asset on the asset profile (or similar work product).
2. Group assets that are collectively needed to perform a specific service, and identify service owners, if necessary.
3. Document and describe the physical location of the asset and the custodian of the asset.

4. Update asset profiles to establish and document the asset's association to a service.

   If the asset is connected to more than one service, be sure this is noted as part of the asset profile.

5. Update the asset database with asset-to-service association information.

   All information relevant to the asset (collected from the asset profile) should be contained with the asset in its entry in the asset database.

ADM:SG2 Establish the Relationship Between Assets and Services

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

The relationship between assets and the services they support must be understood in order to effectively develop, implement, and manage resilience strategies that support the accomplishment of the service's mission. Associating assets to services helps the organization to determine where critical dependencies exist, to validate resilience requirements, and to develop and implement commensurate resilience strategies.

ADM:SG2.SP1 Associate Assets with Services

Assets are associated with the service or services they support.

To provide a service-focused review of operational resilience, the assets collected in the development of the asset inventory must be associated with the services they support. This helps the organization view resilience from a service perspective and to identify critical dependencies that are essential to determining effective strategies for protecting and sustaining assets.

Establishing criteria for determining the relative value of services and associated assets is performed in the Risk Management process area. Identifying and prioritizing high-value organizational services is performed in the Enterprise Focus process area.

Typical work products

1. List of high-value services and associated assets
2. Updated asset profiles (including service information)
3. Updated asset database (including service information)

Subpractices

1. Identify high-value services.

   A list of high-value services is created in the Enterprise Focus process area. Assets can be associated with services in this practice, but it is best to have a validated list of services to which assets are associated. *Refer to the Enterprise Focus process area for more information.*

2. Assign assets in the asset database to one or more services.
3. Update the asset profile to reflect the service association.
4. Update the asset database to reflect the service association.

ADM:SG2.SP2 Analyze Asset-Service Dependencies

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

Because services traverse the organization, and because there are shared assets and resources that many services depend upon, it is important to identify these dependencies to ensure that they are addressed during the development of resilience requirements and in the development of strategies to protect and sustain assets and their related services.

When dependencies result in a shared environment for an asset, consideration must be given to the effects that this situation will have on the satisfaction of resilience requirements at the service level. For example, if resilience requirements are set for a facility and more than one service is performed in that facility, the requirements for protecting and sustaining the facility must be sufficient to meet the needs of both services that share the facility. By identifying these potential conflicts early, an organization can actively mitigate them (by revising requirements or other actions) before they become an exposure that affects the operational resilience of the affected services.

Typical work products

1. List of potential conflicts due to asset dependencies
2. Mitigation actions and resolutions

Subpractices

1. Identify asset dependencies and potential conflicts.
2. Develop mitigation plans to reduce the effects of dependencies that could affect the operational resilience of associated services.
3. Implement actions to reduce or eliminate conflict.

   This practice may require the organization to revisit existing resilience requirements and revise them where necessary. It may also necessitate changes in current strategies for protecting and sustaining existing assets. *Refer to the Resilience Requirements Management process area for more information about managing change to resilience requirements. Refer to the Controls Management and the Service Continuity process areas for managing changes to strategies for protecting and sustaining services and their supporting assets.*

ADM:SG3 Manage Assets

The life cycle of assets is managed.

Changes to high-value assets may require commensurate changes in resilience requirements and the strategies that organizations deploy to ensure that these assets are adequately protected and sustained. In fact, managing changes to the operational environment (i.e., through keeping accurate inventories of assets and services and their requirements) is an essential activity for managing and controlling operational resilience. The organization must actively monitor for changes that significantly alter assets, identify new assets, or call for the retirement of assets for which there is no longer a need or whose relative value has been reduced. The objective of this goal is to ensure

that the organization's scope for operational resilience management remains known and controllable.

ADM:SG3.SP1 Identify Change Criteria

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

(This practice is complementary to specific practice RRM:SG1.SP3 in Resilience Requirements Management.)

In order to identify changes to high-value assets that could affect their productivity and resilience, the organization must have a set of criteria that are consistently applied. These criteria must cover all assets—people, technology, information, and facilities. Changes in assets must be translated to changes in resilience requirements—either the requirements are altered or rewritten, or in the case where the asset is eliminated (for example, when vital staff leave the organization), the requirements are retired.

These are examples of triggers that can affect high-value assets:

- changes in organizational structure and staff—termination or transfer of staff between organizational units or changes in roles and responsibilities
- changes in technology infrastructure and configuration
- real-estate transactions that add, alter, or change existing facilities
- creation or alteration of information
- changes in services affecting the assets on which they rely
- contracts that the organization enters into that would identify new assets
- acquisition of assets such as technology or facilities

Owners of high-value assets must have knowledge of these criteria and be able to apply them in order to identify changes that must be managed.

Typical work products

1. Asset inventory baseline
2. Asset change criteria

Subpractices

1. Establish an asset inventory baseline from which changes will be managed.
2. Develop and document criteria for establishing when a change in asset inventory must be considered.

   Ensure that these criteria are commensurate with the organization's risk tolerances.

ADM:SG3.SP2 Maintain Changes to Assets and Inventory

Changes to assets are managed as conditions dictate.

(This practice is complementary to specific practice RRM:SG1.SP3 in Resilience Requirements Management.)

Organizational and operational conditions are continually changing. These changes result in daily changes to the high-value assets that help the organization's services achieve their missions. For example, the following are common organizational events that would affect high-value assets:

- staff changes, including the addition of new staff members (either internally or externally), the transfer of existing staff members from one organizational unit to another, and the termination of staff members
- changes to information such as the creation, alteration, or deletion of paper and electronic records, files, and databases
- technology refresh, such as the addition of new technical components, changes to existing technical components, and the elimination or retirement of existing technology
- facilities changes, such as the addition of new facilities (whether owned by the organization or an external business partner), alteration of existing facilities, and the retirement of a facility

Besides the addition of new assets, this practice also addresses changes to the description or composition of an asset. For example, if an asset takes an additional form (such as when a paper asset is imaged or an electronic asset is printed), this must be documented as part of the asset description to ensure that current strategies to protect and sustain align properly and provide coverage across a range of asset media. Assets may also change ownership, custodianship, location, or value—all of which must be updated to ensure a current asset profile and inventory.

In addition, whenever assets are eliminated (for example, a server is retired or vital staff members leave the organization), owners of those assets must ensure that their resilience requirements are either eliminated (if possible) or are transferred and updated to the assets that replace them. Doing this is especially critical when assets are shared between services and have common resilience requirements.

Typical work products

1. Asset change documentation
2. Asset inventory status
3. Updated asset and service resilience requirements
4. Updated asset and service protection strategies and controls
5. Updated strategies and continuity plans for sustaining assets and services

Subpractices

1. Document the asset changes by updating asset profiles and the asset database.
2. Maintain a requirement change history with rationale for performing the changes.
3. Evaluate the impact of asset changes on existing resilience requirements and activities and commitments for protecting and sustaining assets.

   Update asset resilience requirements, asset protection strategies, and plans for sustaining assets as necessary.
4. Establish communication channels to ensure custodians are aware of changes in assets.

   Update service level agreements with custodians if necessary to reflect commitment to changes.

Generic Practices by Goal

Refer to the Generic Goals and Practices document for generic goals and practices guidance that applies to all process areas. The generic goals and practices descriptions here provide further details relative to the Asset Definition and Management process area.

ADM:GG1 Achieve Specific Goals

The operational resilience management process supports and enables achievement of the specific goals of the Asset Definition and Management process area by transforming identifiable input work products to produce identifiable output work products.

ADM:GG1.GP1 Perform Asset Definition and Management Practices

Perform the specific practices of the Asset Definition and Management process area to develop work products and provide services to achieve the specific goals of the process area.

Elaboration:

Specific practices ADM:SG1.SP1 through ADM:SG3.SP2 are performed to achieve the goals of the asset definition and management process.

ADM:GG2 Institutionalize Asset Definition and Management as a Managed Process

Asset definition and management is institutionalized as a managed process.

ADM:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the asset definition and management process.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the asset definition and management process.

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the asset definition and management process may be exhibited by

   - developing and publicizing higher level managers' objectives and requirements
   - sponsoring policies, procedures, standards, and guidelines, including the documentation of assets and for establishing asset ownership and custodianship
   - making higher level managers aware of applicable compliance obligations related to the process, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
   - sponsoring and funding process activities
   - aligning asset inventory, asset ownership, and asset-service relationship activities with identified resilience needs and objectives and stakeholder needs and requirements
   - sponsoring the development, documentation, and management of asset inventories
   - verifying that the process supports strategic resilience objectives and is focused on the assets and services that are of the highest relative value in meeting strategic objectives
   - regular reporting from organizational units to higher level managers on process activities and results
   - creating dedicated higher level management feedback loops on decisions about the process and recommendations for improving the process
   - providing input on identifying, assessing, and managing operational risks to assets, including guidance for resolving asset inventory inconsistencies and other anomalies
   - conducting regular internal and external audits and related reporting to audit committees on process effectiveness
   - creating formal programs to measure the effectiveness of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

Elaboration:

The asset definition and management policy should address

- responsibility, authority, and ownership for performing process activities, including collecting and documenting asset inventory information
- procedures, standards, and guidelines for
  - documenting asset descriptions and relevant information
  - describing and identifying asset owners
  - describing and identifying asset custodians
- the development of criteria to provide guidance on asset inventory updating, reconciliation, and change control
- the association of assets to core organizational services, and the prioritization of assets in the inventory
- methods for measuring adherence to policy, exceptions granted, and policy violations

ADM:GG2.GP2 Plan the Asset Definition and Management Process

Establish and maintain the plan for performing the asset definition and management process.

Elaboration:

The plan for performing the asset definition and management process is created to ensure that an accurate inventory of assets is developed and maintained and can form a foundation for managing operational resilience. Developing and maintaining an asset inventory may be challenging because most organizations have a significant number of assets. Thus, the plan must address how the inventory will be taken and maintained at various levels of the organization. For practicality, most organizations may take inventory at an organizational unit level and have a method or tool to aggregate the inventory at an enterprise level.

Subpractices

1. Define and document the plan for performing the process.

   Elaboration:

   Special consideration in the plan may need to be given to the organization's approach for taking an initial inventory of assets (developing the asset inventory baseline) and for maintaining the asset inventory. The plan should address who is responsible for creating and maintaining the inventory and how ownership and custodianship is determined (or assigned). The plan should also include provisions for how the inventory is to be reconciled and how inventory duplication is resolved.

2. Define and document the process description.
3. Review the plan with relevant stakeholders and get their agreement.
4. Revise the process plan as necessary.

ADM:GG2.GP3 Provide Resources

Provide adequate resources for performing the asset definition and management process, developing the work products, and providing the services of the process.

Subpractices

1. Staff the process.

   Elaboration:

   The diversity of asset types (people, information, technology, facilities) requires that staff members assigned to the asset definition and management process have appropriate knowledge of the assets being inventoried and the services with which they are associated.

   These are examples of staff required to perform the asset definition and management process:

   - staff responsible for
     - identifying high-value assets (e.g., people, information, technology, and facilities) and the services with which they are associated
     - developing and maintaining the asset inventory, including asset profiles and the asset database
     - identifying asset dependencies, potential conflicts, and mitigation plans to reduce the effects of dependencies that could affect the operational resilience of associated services
     - managing changes to assets, changes to the asset inventory, and associated changes to requirements, controls, strategies, and plans. This includes communicating changes to affected stakeholders, including asset custodians.
     - developing process plans and programs and ensuring they are aligned with stakeholder requirements and needs
     - managing external entities that have contractual obligations for asset definition and management activities
   - owners and custodians of high-value assets that support the accomplishment of operational resilience management objectives
   - internal and external auditors responsible for reporting to appropriate committees on process effectiveness

   Refer to the Organizational Training and Awareness process area for information about training staff for resilience-focused roles and responsibilities.

   Refer to the Human Resource Management process area for information about acquiring staff to fulfill roles and responsibilities.

2. Fund the process.

   Elaboration:

   Considerations for funding the asset definition and management process should extend beyond the initial development of the asset inventory to the maintenance of the inventory. Initial costs may be higher if the organization does not have a formal or usable asset baseline to serve as a foundation.

   Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for service continuity.

3. Provide necessary tools, techniques, and methods to perform the process.

   Elaboration:

   Developing and maintaining the asset inventory may require tools, techniques, and methods that allow for asset documentation and profiling, reporting, and updating on a regular basis. The need for these tools may be greater if the asset inventory is developed across many organizational units and must be aggregated at the enterprise level. Tools should provide for proper and secure change control over the asset database and should limit access to the asset baseline. The asset inventory database should be searchable and expandable to include additional information such as documentation of associated services and the asset's resilience requirements.

   These are examples of tools, techniques, and methods for asset definition and management:

   - methods for identifying high-value assets
   - methods, techniques, and tools for creating asset profiles and baselines
   - methods and tools for aggregating local asset inventories into an enterprise inventory
   - asset inventory database management system
   - methods, techniques, and tools for asset inventory change management and control

ADM:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the asset definition and management process, developing the work products, and providing the services of the process.

Elaboration:

Specific practice ADM:SG1.SP2 describes the use of human resources databases to identify roles of vital staff to aid in determining high-value people assets. Specific practice ADM:SG1.SP2 calls for describing roles rather than actual persons that perform the role. Specific practice ADM:SG3.SP1 discusses the effects of changes in roles. These descriptions of roles specific to the definition and management of high-value people assets should not be confused with assigning the roles, responsibilities, and authorities necessary to perform the asset definition and management process.

Refer to the Human Resource Management process area for more information about establishing resilience as a job responsibility, developing resilience-related performance goals and objectives, and measuring and assessing performance against goals and objectives.

Subpractices

1. Assign responsibility and authority for performing the process.

   Elaboration:

   Responsibility and authority for creating the asset inventory baseline may differ from responsibility and authority for maintaining the asset inventory and performing change control processes.

2. Assign responsibility and authority for performing the specific tasks of the process.

   Elaboration:

   Responsibility and authority for performing asset definition and management tasks can be formalized by

   - defining roles and responsibilities in the process plan
   - including process tasks and responsibility for these tasks in specific job descriptions
   - developing policy requiring organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in and derive benefit from the process for assets and services under their ownership or custodianship
   - including process tasks in employee performance management goals and objectives with requisite measurement of progress against these goals
   - developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions
   - including process tasks in measuring performance of external entities against contractual instruments

   Refer to the External Dependencies Management process area for additional details about managing relationships with external entities.

3. Confirm that people assigned with responsibility and authority understand it and are willing and able to accept it.

ADM:GG2.GP5 Train People

Train the people performing or supporting the asset definition and management process as needed.

Refer to the Organizational Training and Awareness process area for more information about training the people performing or supporting the process.

Refer to the Human Resource Management process area for more information about creating an inventory of skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.

   Elaboration:

   These are examples of skills required in the asset definition and management process:

   - knowledge of the tools, techniques, and methods necessary to identify and inventory high-value assets. This includes those necessary to perform the process using the selected methods, techniques, and tools identified in ADM:GG2.GP3 subpractice 3.
   - knowledge unique to each type of asset that is required to identify and inventory each type
   - knowledge necessary to work effectively with asset owners and custodians
   - knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective requirements, plans, and programs for the process

2. Identify process skill gaps based on available resources and their current skill levels.

3. Identify training opportunities to address skill gaps.

   Elaboration:

   These are examples of training topics:

   - profiling, defining, and documenting high-value assets, including any unique considerations by asset type
   - managing and controlling changes to asset inventories, asset profiles, and asset databases
   - supporting asset owners and custodians in understanding the process and their roles and responsibilities with respect to its activities
   - working with external entities who have responsibility for process activities
   - using process methods, tools, and techniques, including those identified in ADM:GG2:GP3 subpractice 3

4. Provide training and review the training needs as necessary.

ADM:GG2.GP6 Manage Work Product Configurations

Place designated work products of the asset definition and management process under appropriate levels of control.

Elaboration:

ADM:SG3.SP2 specifically addresses the change control process over assets and the asset inventory. However, other work products of the asset definition and management process must also be managed and controlled.

The tools, techniques, and methods used to capture and maintain the asset inventory should be employed to perform consistent and structured version control over the inventory to ensure that information is current, accurate, and "official." The tools, techniques, and methods can also be used to securely store the asset inventory, provide access control over inquiry, modification, and deletion, and to track version changes and updates.

These are examples of asset definition and management work products placed under control:

- asset inventory
- asset database
- asset profiles
- asset owners and custodians
- association of assets to high-value services
- asset dependencies, dependency conflicts, mitigation actions, and resolutions
- asset inventory change control system or method
- asset inventory change criteria
- process plan
- policies and procedures
- contracts with external entities

ADM:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the asset definition and management process as planned.

Elaboration:

Several ADM specific practices address the involvement of owners and custodians as key stakeholders in the asset definition and management process. For example, ADM:SG1.SP3 calls for establishing ownership and custodianship for all high-value assets and making sure owners and custodians understand their responsibilities, as well as their relationship with one another. ADM:SG3.SP1 requires that asset owners have knowledge of asset change criteria, including possible changes in asset ownership and custodianship.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the asset definition and management process:

   - asset owners and custodians
   - service owners
   - organizational unit and line of business managers responsible for high-value assets and the services they support
   - staff responsible for establishing, implementing, and maintaining an internal control system for assets
   - external entities responsible for managing high-value assets
   - human resources (for people assets)
   - information technology staff (for technology assets)
   - staff responsible for physical security (for facility assets)
   - internal and external auditors

   Stakeholders are involved in various tasks in the asset definition and management process, such as

   - planning for the process
   - creating an asset inventory baseline
   - creating asset profiles
   - associating assets with services and analyzing asset-service dependencies
   - managing changes to assets and to the asset inventory
   - reviewing and appraising the effectiveness of process activities
   - resolving issues in the process

2. Communicate the list of stakeholders to planners and those responsible for process performance.
3. Involve relevant stakeholders in the process as planned.

ADM:GG2.GP8 Monitor and Control the Process

Monitor and control the asset definition and management process against the plan for performing the process and take appropriate corrective action.

Refer to the Monitoring process area for more information about the collection, organization, and distribution of data that may be useful for monitoring and controlling processes.

Refer to the Measurement and Analysis process area for more information about establishing process metrics and measurement.

Refer to the Enterprise Focus process area for more information about providing process information to managers, identifying issues, and determining appropriate corrective actions.

Subpractices

1. Measure actual performance against the plan for performing the process.
2. Review accomplishments and results of the process against the plan for performing the process.

   Elaboration:

   These are examples of metrics for the asset definition and management process:

   - percentage of organizational assets that have been inventoried, by asset type
   - number or level of discrepancies between the current inventory and the documented inventory
   - number of changes made to the asset inventory during a stated period
   - number of assets that do not have an assigned owner or custodian (if applicable)
   - number of assets with incomplete asset profiles or other incomplete information
   - number of asset-service dependency conflicts with unimplemented or incomplete mitigation plans
   - number of high-value asset risks referred to the risk management process; number of risks where corrective action is still pending (by risk rank)
   - level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved
   - number of process activities that are on track per plan
   - rate of change of resource needs to support the process
   - rate of change of costs to support the process

3. Review activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues.

   Elaboration:

   Periodic reviews of the asset definition and management process are needed to ensure that

   - newly acquired assets are included in the inventory
   - assets that have been modified are reflected accurately in the inventory
   - assets that have been retired are removed from the inventory
   - asset-service mapping is accurate and current
   - ownership and custodianship over assets are established and documented
   - change control processes are operating appropriately to minimize discrepancies between the organization's asset base and the asset inventory
   - access to the asset inventory is being limited to only authorized staff
   - status reports are provided to appropriate stakeholders in a timely manner
   - asset and service dependency issues are referred to the risk management process when necessary
   - actions requiring management involvement are elevated in a timely manner
   - the performance of process activities is being monitored and regularly reported
   - key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
   - administrative, technical, and physical controls are operating as intended
   - controls are meeting the stated intent of the resilience requirements
   - actions resulting from internal and external audits are being closed in a timely manner

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.

   Elaboration:

   Discrepancies result when assets are acquired, modified, or retired but not reflected accurately in the asset inventory. Assets form the foundation for operational resilience management, as they are the target of strategies required to protect and sustain services. To the extent that the asset definition and management process results in inventory discrepancies, the organization's overall ability to manage operational resilience is impeded.

5. Identify problems in the plan for performing and executing the process.
6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.
7. Track corrective action to closure.

ADM:GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the process against its process description, standards, and procedures, and address noncompliance.

Elaboration:

These are examples of activities to be reviewed:

- identifying assets and services
- associating assets and services
- identifying asset-service dependencies
- developing asset profiles
- documenting asset descriptions
- identifying asset change criteria
- making changes to the asset inventory
- the alignment of stakeholder requirements with process plans
- assignment of responsibility, accountability, and authority for process activities
- determination of the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action if any
- verification of process controls
- use of process work products for improving strategies to protect and sustain assets and services

These are examples of work products to be reviewed:

- asset profiles
- asset inventory database
- asset-service relationship matrix
- asset inventory change control logs
- process plan and policies
- dependency issues that have been referred to the risk management process
- process methods, techniques, and tools
- contracts with external entities
- metrics for the process *(refer to ADM:GG2.GP8 subpractice 2)*

ADM:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the process with higher level managers and resolve issues.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management process.

ADM:GG3 Institutionalize Asset Definition and Management as a Defined Process

Asset definition and management is institutionalized as a defined process.

ADM:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined asset definition and management process.

Establishing and tailoring process assets, including standard processes, is addressed in the Organizational Process Definition process area.

Establishing process needs and objectives and selecting, improving, and deploying process assets, including standard processes, is addressed in the Organizational Process Focus process area.

Subpractices

1. Select from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization's tailoring guidelines.
3. Ensure that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.
5. Revise the description of the defined process as necessary.

ADM:GG3.GP2 Collect Improvement Information

Collect asset definition and management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.

Elaboration:

These are examples of improvement work products and information:

- asset inventory
- conflicts arising from asset-service relationships
- metrics and measurements of the viability of the process *(refer to ADM:GG2.GP8 subpractice 2)*
- changes and trends in operating conditions, risk conditions, and the risk environment that affect process results
- lessons learned in post-event review of incidents and disruptions in continuity
- process lessons learned that can be applied to improve operational resilience management performance, such as poorly documented or profiled assets and difficulties in assigning and executing asset ownership and custodianship responsibilities
- the level to which the asset inventory, asset profiles, and the asset database reflect the current status of all assets
- reports on controls effectiveness and weaknesses, including issues related to change control on the asset inventory
- asset-service dependency mitigation plans that are not executed and the risks associated with them
- resilience requirements that are not being satisfied or are being exceeded

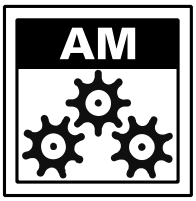
Establishing the measurement repository and process asset library is addressed in the Organizational Process Definition process area. Updating the measurement repository and process asset library as part of process improvement and deployment is addressed in the Organizational Process Focus process area.

Subpractices

1. Store process and work product measures in the organization's measurement repository.
2. Submit documentation for inclusion in the organization's process asset library.
3. Document lessons learned from the process for inclusion in the organization's process asset library.
4. Propose improvements to the organizational process assets.

ACCESS MANAGEMENT

Operations



Purpose

The purpose of Access Management is to ensure that access granted to organizational assets is commensurate with their business and resilience requirements.

Introductory Notes

In order to support services, assets such as information, technology, and facilities must be made available (accessible) for use. This requires that persons (employees and contractors), objects (such as systems), and entities (such as business partners) have sufficient (but not excessive) levels of access to these assets.

Effective access management requires balancing organizational needs against the appropriate level of controls based on an asset's resilience requirements and business objectives. Insufficient access may translate into higher levels of asset protection but may impede the organization's ability to use the assets to their productive capacity. On the other hand, excessive levels of access (due to inadequate levels of control) expose assets to potential unauthorized or inadvertent misuse, which may diminish their productive capacity. Finding the right level of access for persons, objects, and entities so that they can perform their job responsibilities while satisfying the protection needs for the asset is a process that involves business owners, organizational units, and the owners and custodians of assets. In essence, these parties must come to agreement on what level of protection is sufficient given the need to meet objectives. Access management encompasses the processes that the organization uses to address this balancing act.

Access privileges and restrictions are the mechanism for linking persons, objects, and entities (and their organizational roles) to the assets they need to perform their responsibilities. Access privileges and restrictions are operationalized (i.e., made operational or implemented) through logical and physical *access controls*, which may be administrative, technical, or physical in nature and can be discretionary (i.e., at the will of the asset owner) or mandatory (constrained by policies, regulations, and laws).

Access controls differ significantly from access privileges and restrictions. In the purest sense, an access control is the administrative, technical, or physical mechanism that provides a gate at which identities must present proper credentials to pass. Some examples of access controls are access and security policies, access control lists in application systems and databases, and key card and key pad readers for facilities. Access controls are established relative to the resilience requirements for an asset and service they protect—they are the mechanism that enforces the resilience requirements of confidentiality, integrity, and availability. When an identity presents an access request to an access control, and the identity has the necessary credentials required by the control (i.e., is authenticated and authorized to have the level of access requested), access is provided.

Access controls are a key element of the protection provided to an asset and form a substantial portion of the organization's protection strategy for assets and services. Because the operational environment is constantly changing, it is difficult for an organization to keep

access controls current and reflective of actual business and resilience requirements. The Access Management process area establishes processes to ensure that access to organizational assets remains consistent with the business and resilience requirements of those assets even as the organization's operating environment changes. At a summary level, this includes activities to

- involve owners of assets in the process of establishing and maintaining access privileges
- manage changes to access privileges as the identities, user roles, business requirements, and resilience requirements change
- monitor and analyze relationships between identities, roles, and current access privileges to ensure alignment with business and resilience requirements
- adjust access privileges when they are not aligned with business and resilience requirements
- ensure that the access privileges granted to a user by the system of access controls reflect the privileges assigned by the asset owner

Clearly, access management is strongly tied to identity management. In identity management, persons, objects, and entities are established as identities that may require some level of access to organizational assets. However, access privileges and restrictions are tied to identities by the roles that are attributed to the identity. Thus, as identities change, or as their roles change, there is a cascading effect on access privileges that must be managed. For example,

- new identities may be established that must be provided access privileges
- the access privileges of existing identities may have to be changed as the job responsibilities associated with the identity change
- the access privileges of existing identities may need to be eliminated or deprovisioned as job responsibilities expire (either through new assignments or voluntary or involuntary termination)

The selection of the appropriate access controls to enforce those rights for a given asset is outside of the scope of this process area. These activities are performed in the operations process area associated with each type of asset (e.g., Knowledge and Information Management for information assets). Overall management of the organization's internal control system is addressed in the Controls Management process area.

Related Process Areas

The creation, maintenance, and deprovisioning of identities and their associated attributes is addressed in the Identity Management process area.

The selection and implementation of appropriate access controls for assets is addressed in the Knowledge and Information Management process area (for information), Technology Management process area (for technology assets), and the Environmental Control process area (for facilities).

The analysis and mitigation of risks related to inappropriate or excessive levels of access privileges is addressed in the Risk Management process area.

Summary of Specific Goals and Practices

Goals	Practices
AM:SG1 Manage and Control Access	AM:SG1.SP1 Enable Access
	AM:SG1.SP2 Manage Changes to Access Privileges
	AM:SG1.SP3 Periodically Review and Maintain Access Privileges
	AM:SG1.SP4 Correct Inconsistencies

Specific Practices by Goal

AM:SG1 Manage and Control Access

Access granted to organizational assets is managed and controlled.

AM:SG1.SP1 Enable Access

Appropriate access to organizational assets is informed by resilience requirements and owner approval.

AM:SG1.SP2 Manage Changes to Access Privileges

Manage changes to access privileges as assets, roles, and resilience requirements change.

AM:SG1.SP3 Periodically Review and Maintain Access Privileges

Periodic review is performed to identify excessive or inappropriate levels of access privileges.

AM:SG1.SP4 Correct Inconsistencies

Excessive or inappropriate levels of access privileges are corrected.

COMMUNICATIONS

Enterprise

Purpose

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

Introductory Notes

Communication is a basic organizational activity and competency. From a resilience perspective, communication is an essential function, tying together disparate parts of the organization that collectively have a vested interest in protecting high-value assets and services and sustaining assets and services during and after a disruptive event.

Internally, communication processes are embedded in operational resilience management processes such as incident management, governance, and compliance, and support the development and execution of plans for sustaining the required level of resilience; externally, communication processes provide much needed information to relevant stakeholders on the capability of the organization to protect and sustain assets and services, handle disruptions, and preserve customer confidence in unsettled and stressful times. Most importantly, communications are a critical success factor in ensuring the successful execution of service continuity plans and decision making, particularly during a crisis or disaster.

The Communications process area seeks to capture the communications activities that support and enable effective management of operational resilience. This requires foundational processes for basic and ongoing communications needs as well as more flexible ones for supporting the communications demands of managing events and executing service continuity plans. In the Communications process area, the organization establishes communications requirements that reflect the needs of stakeholders that are important to managing operational resilience. Communications guidelines and standards are developed to ensure the consistency and accuracy of messages and communication methods across all resilience processes. The communications infrastructure is established and managed to ensure effective and continuous communications flow when needed. The organization also regularly assesses its communications abilities, particularly after an event, incident, or crisis, to revise communications requirements and to make improvements in the type and media of communications and the communications infrastructure.

The Communications process area focuses on communications processes that directly support the management of operational resilience. These processes are likely to be part of a larger (and in some cases, enterprise-wide) communications process in the organization. Thus, the Communications process area is not considered a substitute for this larger process.

Related Process Areas

The definition of the resilience program and the development of program objectives is established in the Enterprise Focus process area.

The data and information that the organization needs to provide governance and control over the operational resilience management program is established in the Monitoring process area and used in the Enterprise Focus process area.

The guidelines and standards for communicating about events, incidents, and crises are addressed in the Incident Management and Control process area.

The guidelines and standards for communicating with external entities to coordinate management of events are addressed in the External Dependencies Management process area.

Specific communications activities relevant to service continuity plans are developed and implemented in the Service Continuity process area.

Awareness communications relative to operational resilience management are addressed in the Organizational Training and Awareness process area.

Summary of Specific Goals and Practices

Goals	Practices
COMM:SG1 Prepare for Resilience Communications	COMM:SG1.SP1 Identify Relevant Stakeholders
	COMM:SG1.SP2 Identify Communications Requirements
	COMM:SG1.SP3 Establish Communications Guidelines and Standards
COMM:SG2 Prepare for Communications Management	COMM:SG2.SP1 Establish a Resilience Communications Plan
	COMM:SG2.SP2 Establish a Resilience Communications Program
	COMM:SG2.SP3 Identify and Assign Plan Staff
COMM:SG3 Deliver Resilience Communications	COMM:SG3.SP1 Identify Communications Methods and Channels
	COMM:SG3.SP2 Establish and Maintain Communications Infrastructure
COMM:SG4 Improve Communications	COMM:SG4.SP1 Assess Communications Effectiveness
	COMM:SG4.SP2 Improve Communications

Specific Practices by Goal

COMM:SG1 Prepare for Resilience Communications

The requirements, guidelines, and standards for resilience communications are established.

COMM:SG1.SP1 Identify Relevant Stakeholders

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

COMM:SG1.SP2 Identify Communications Requirements

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

COMM:SG1.SP3 Establish Communications Guidelines and Standards

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

COMM:SG2 Prepare for Communications Management

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

COMM:SG2.SP1 Establish a Resilience Communications Plan

Planning for the resilience communications process is performed.

COMM:SG2.SP2 Establish a Resilience Communications Program

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

COMM:SG2.SP3 Identify and Assign Plan Staff

Staff are assigned authority and accountability for carrying out the communications plan and program.

COMM:SG3 Deliver Resilience Communications

The activities necessary to deliver communications for resilience activities on an operational and event-driven basis are established.

COMM:SG3.SP1 Identify Communications Methods and Channels

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

COMM:SG3.SP2 Establish and Maintain Communications Infrastructure

An infrastructure appropriate to meet the organization's resilience communication needs is established and managed.

COMM:SG4 Improve Communications

Resilience communications are reviewed to identify and implement improvements in the communications process.

COMM:SG4.SP1 Assess Communications Effectiveness

The effectiveness of resilience communications plans and programs are assessed and corrective actions are identified.

COMM:SG4.SP2 Improve Communications

Lessons learned in managing resilience communications are used to improve communications plans and programs.

COMPLIANCE

Enterprise

Purpose

The purpose of Compliance is to ensure awareness of and compliance with an established set of relevant internal and external guidelines, standards, practices, policies, regulations, and legislation, and other obligations (such as contracts and service level agreements) related to managing operational resilience.

Introductory Notes

Regulations, standards, and guidelines are developed and issued by a variety of governmental, regulatory, and industry bodies. Their purpose is to enforce (and reinforce) acceptable levels of behavior to ensure that organizations and the services they provide to citizens and customers remain viable and sustainable. In particular, the evolving importance of security and resilience has resulted in a new wave of regulatory bodies and regulations that seek not only to ensure organizational survivability but the survivability of entire industries and to limit undesirable events that have the potential to affect the socioeconomic structure of the global economy.

“Compliance” characterizes the activities that the organization performs to identify the internal and external guidelines, standards, practices, policies, regulations, and legislation to which it is subject and to comply with these obligations in an orderly, systematic, efficient, timely, and accurate manner. Compliance management addresses the policies and practices in the organization that support the satisfaction of compliance obligations as an enterprise-wide activity that involves more than just legal and administrative activities.

Organizations typically focus their efforts on compliance with externally directed obligations, but compliance processes also often address compliance with internally generated standards and policies such as the organization’s information security policy and internal control system. In addition, compliance is not only important for reinforcing appropriate behaviors; it is also a primary tool in governing the security and resilience activities in the organization and ensuring they are effectively meeting their goals and objectives.

The Compliance process area addresses the organization’s ability to establish a compliance plan and program, to identify relevant regulations, standards, and guidelines (to which it must comply), and to develop and implement the proper procedures and activities to ensure compliance in a timely and accurate manner. Compliance management requires the organization to understand its obligations and to collect relevant data in a manner that supports and enables the satisfaction of obligations in a way that meets the organization’s requirements but does not divert focus from its core service delivery.

Related Process Areas

A primary component of the compliance process—governance and oversight—is addressed in the Enterprise Focus process area.

Addressing the risks of non-compliance and the risks related to weaknesses identified in the compliance process is performed in the Risk Management process area.

The monitor process, which may provide information about the effectiveness of internal controls for compliance purposes, is addressed in the Monitoring process area.

Summary of Specific Goals and Practices

Goals	Practices
COMP:SG1 Prepare for Compliance Management	COMP:SG1.SP1 Establish a Compliance Plan
	COMP:SG1.SP2 Establish a Compliance Program
	COMP:SG1.SP3 Establish Compliance Guidelines and Standards
COMP:SG2 Establish Compliance Obligations	COMP:SG2.SP1 Identify Compliance Obligations
	COMP:SG2.SP2 Analyze Obligations
	COMP:SG2.SP3 Establish Ownership for Meeting Obligations
COMP:SG3 Demonstrate Satisfaction of Compliance Obligations	COMP:SG3.SP1 Collect and Validate Compliance Data
	COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction
	COMP:SG3.SP3 Remediate Areas of Non-Compliance
COMP:SG4 Monitor Compliance Activities	COMP:SG4.SP1 Evaluate Compliance Activities

Specific Practices by Goal

COMP:SG1 Prepare for Compliance Management

The organizational environment and processes for identifying, satisfying, and monitoring compliance obligations are established.

COMP:SG1.SP1 Establish a Compliance Plan

A strategic plan for managing compliance to obligations is established.

COMP:SG1.SP2 Establish a Compliance Program

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

COMP:SG1.SP3 Establish Compliance Guidelines and Standards

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

COMP:SG2 Establish Compliance Obligations

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

COMP:SG2.SP1 Identify Compliance Obligations

Compliance obligations are identified and documented.

COMP:SG2.SP2 Analyze Obligations

Compliance obligations are analyzed and organized to facilitate satisfaction.

COMP:SG2.SP3 Establish Ownership for Meeting Obligations

The responsibility for satisfying compliance obligations is established.

COMP:SG3 Demonstrate Satisfaction of Compliance Obligations

The organization demonstrates that its compliance obligations are being satisfied.

COMP:SG3.SP1 Collect and Validate Compliance Data

Data required to satisfy compliance obligations is collected and validated.

COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction

The extent to which compliance obligations are satisfied is demonstrated through compliance activities.

COMP:SG3.SP3 Remediate Areas of Non-Compliance

Remediation of areas of non-compliance is performed to ensure satisfaction of compliance obligations.

COMP:SG4 Monitor Compliance Activities

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

COMP:SG4.SP1 Evaluate Compliance Activities

Satisfaction of the organization's compliance obligations is independently monitored and improved.

CONTROLS MANAGEMENT

Engineering

Purpose

The purpose of Controls Management is to establish, monitor, analyze, and manage an internal control system that ensures the effectiveness and efficiency of operations through assuring mission success of high-value services and the assets that support them.

Introductory Notes

Internal control is a governance process used by the organization to ensure effective and efficient achievement of organizational objectives and to provide reasonable assurance of success. The internal control process is pervasive throughout the organizational structure from higher level managers to staff and is reflected in all levels of operations—in many cases, down to the transaction level.

The organization's high-level managers have the responsibility to set the tone for internal control so that the objectives of the organization are reflected in all operational activities. In this way, the organization ensures success by building in success criteria at all operational levels.

The internal control process is typically reflected in the organization's *internal control system*. By definition, the internal control system is the aggregation of the activities an organization undertakes to ensure success. While this is primarily operational in implementation, there are other broad objectives of the internal control system, including promoting ethical behavior, preventing and detecting fraud, ensuring compliance with laws and regulations, and providing more predictability in the overall performance of the organization. At the operational level, the internal control system is the aggregation of the policies, procedures, methods, technologies, and tools that provide assurance that management directives are carried out. For example, an organization may find it vital to its profitability that all intellectual property be kept confidential and only provided to staff who have a justifiable need-to-know. Thus, a policy may be drafted that provides guidance on the effective handling and distribution of this information. The policy is a means for implementing management's directives and minimizing impact on organizational success and achievement.

Internal control in a broad sense is focused on ensuring that the financial condition of an organization is accurately reflected in its financial and accounting records. However, at an operational level, internal control relates to implementing policies, procedures, methods, technologies, and tools that support service mission assurance. Typically this involves the development of high-level control objectives that align with service mission assurance requirements and strategies to protect and sustain services that satisfy these requirements. Control objectives are then translated into appropriate policies, procedures, methods, technologies, and tools—referred to as operational controls—that are needed to meet each objective. From an operational resilience management perspective, these operational controls are critical to protecting assets, sustaining assets, and preventing disruption to assets as they are deployed in the execution of a service. That said, effective controls management for operational resilience means identifying the most cost-effective strategies

for protecting and sustaining assets and services. The organization should seek the optimum mix in contrast to, for example, deploying an extensive number of overlapping and redundant controls in reaction to new compliance requirements.

In the Controls Management process area, the organization establishes control objectives that reflect the organization's objectives and mission and defines the target for the development of enterprise and operational-level controls. Enterprise controls are developed to address organization-wide directives that universally affect all operational layers. Operational controls are developed, implemented, monitored, analyzed, and managed at the services level to ensure services meet their mission and, specifically, that assets related to services are protected from disruption. These controls may be administrative, technical, or physical in nature and typically are implemented in layers to reinforce strategies to protect and sustain assets and to meet control objectives. Enterprise and operational controls are analyzed and validated to ensure that they meet control objectives as implemented; gaps in effectiveness are identified on a periodic basis and addressed so that control objectives are attained on a consistent basis. It should be noted that the internal control environment in an organization is vast; however, in Controls Management the focus is on controls that relate directly to the deployment of people and the use of information, technology, and facilities in executing services. Depending on the organization, this may include administrative controls, such as separation of duties, or more specific controls, such as the implementation of a physical access control system at a facility. In other words, the subset of operational controls used by the organization to ensure operational resilience is specific to the high-value services that the organization relies on to carry out its mission. Thus, this subset is likely only a small part of the organization's overall internal control system.

The Controls Management and Service Continuity process areas establish the range of controls necessary to ensure that services meet their missions even when disrupted. Controls Management focuses on controls that support protection and sustainment strategies—those that help to prevent services and assets from exposure to vulnerabilities and threats and those that help services and assets respond and recover when disrupted. However, all threat conditions cannot be known or anticipated. Service Continuity also focuses on sustaining services and assets under degraded conditions and in returning them to a normal operating state when possible. Service Continuity is also important because controls that have been implemented may not always meet control objectives, or may not be operating effectively. In these cases, until control remediation actions can occur, the service continuity process sustains services and their supporting assets in the near term.

Related Process Areas

Strategic goals, objectives, critical success factors, and governance for operational resilience management process, as well as the identification of high-value services, are addressed in the Enterprise Focus process area.

Identification, analysis, and mitigation strategies for operational risks are addressed in the Risk Management process area.

Ensuring compliance with identified obligations related to managing operational resilience, including those satisfied by the internal control system, is addressed in the Compliance process area.

The relationship between assets and services is established in the Asset Definition and Management process area.

The identification and implementation of controls for information assets is performed in the Knowledge and Information Management process area.

The identification and implementation of controls for facilities is performed in the Environmental Control process area.

The identification and implementation of controls for technology assets is performed in the Technology Management process area.

Controls related to establishing and managing the contributions and availability of people are identified and implemented in the People Management process area.

The development of service continuity plans as a control for protecting and sustaining services and assets is addressed in the Service Continuity process area.

Monitoring the internal control system for the operational resilience management process is addressed in the Monitoring process area.

Supporting information needs for managing the internal control system in support of operational resilience is addressed in the Measurement and Analysis process area.

Summary of Specific Goals and Practices

Goals	Practices
CTRL:SG1 Establish Control Objectives	CTRL:SG1.SP1 Define Control Objectives
CTRL:SG2 Establish Controls	CTRL:SG2.SP1 Define Controls
CTRL:SG3 Analyze Controls	CTRL:SG3.SP1 Analyze Controls
CTRL:SG4 Assess Control Effectiveness	CTRL:SG4.SP1 Assess Controls

Specific Practices by Goal

CTRL:SG1 Establish Control Objectives

Organizational objectives to be achieved through the selection and implementation of controls are established.

CTRL:SG1.SP1 Define Control Objectives

Control objectives are established as the basis for the selection, implementation, and management of the organization's internal control system.

CTRL:SG2 Establish Controls

Controls that support control objectives and strategies for protecting and sustaining high-value services and assets are established.

CTRL:SG2.SP1 Define Controls

Controls that protect services and assets from disruption are identified and established.

CTRL:SG3 Analyze Controls

Controls are analyzed to ensure they satisfy control objectives.

CTRL:SG3.SP1 Analyze Controls

Controls are analyzed to determine their ability to achieve control objectives.

CTRL:SG4 Assess Control Effectiveness

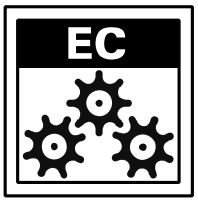
The ability of the internal control system to satisfy resilience requirements is assessed.

CTRL:SG4.SP1 Assess Controls

Controls are assessed for effectiveness in meeting control objectives and satisfying resilience requirements.

ENVIRONMENTAL CONTROL

Operations



Purpose

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

Introductory Notes

Facilities are a subset of the physical plant assets of the organization that are relied upon to execute a service. They are hubs of activity where many of the organization's services intersect, such as office buildings and warehouses. Facilities can be owned by the organization but just as often are leased from an external provider, and they may even encompass workers' homes and other locations where high-value services are physically executed.

People, information, and technology assets "live" within a physical facility—they provide the physical space for the actions of people (people work in offices), the use and storage of information (such as in file rooms and on servers), and the operation of technology components (such as in data centers and server farms). Because of its nature as an activity hub, when a facility is disrupted, there is often a widespread cascading effect on the operability of these other assets, impacting mission assurance of associated services and possibly translating to a failure to achieve organizational goals and objectives.

As a complicating factor, organizations frequently execute their services in facilities that they do not own or control. These arrangements sometimes also mean that the organization's assets are co-located with the assets of other organizations. This presents challenges not only for facilities management but for ensuring the operational resilience of services that depend on these facilities to meet their missions.

The Environmental Control process area addresses the importance of facilities in the operational resilience of services as well as the unique issues that facility assets inherit because of their geographical location and the environment in which they operate. In this process area, facility assets are prioritized according to their value in supporting high-value organizational services. Physical, technical, and administrative controls that sustain the operational viability of facility assets are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, facility risks are identified and mitigated in an attempt to prevent disruption where possible. Because facilities are intricately tied to the geographical location in which they operate, the unique dependencies of the facility on its adjacent environment are identified and actively managed.

Related Process Areas

The establishment and management of resilience requirements for facility assets is performed in the Resilience Requirements Development and Resilience Requirements Management process areas.

The identification, definition, and management of facility assets is addressed in the Asset Definition and Management process area.

The risk management cycle for facility assets is addressed in the Risk Management process area.

The management of the internal control system that ensures the protection of facility assets is addressed in the Controls Management process area.

The selection, implementation, and management of access controls for facility assets is performed in the Access Management process area.

The development of service continuity plans for facilities is performed in the Service Continuity process area.

The establishment and management of relationships with external entities to ensure the resilience of services that are executed in facilities they own and operate is addressed in the External Dependencies Management process area.

Summary of Specific Goals and Practices

Goals	Practices
EC:SG1 Establish and Prioritize Facility Assets	EC:SG1.SP1 Prioritize Facility Assets
	EC:SG1.SP2 Establish Resilience-Focused Facility Assets
EC:SG2 Protect Facility Assets	EC:SG2.SP1 Assign Resilience Requirements to Facility Assets
	EC:SG2.SP2 Establish and Implement Controls
EC:SG3 Manage Facility Asset Risk	EC:SG3.SP1 Identify and Assess Facility Asset Risk
	EC:SG3.SP2 Mitigate Facility Risks
EC:SG4 Control Operational Environment	EC:SG4.SP1 Perform Facility Sustainability Planning
	EC:SG4.SP2 Maintain Environmental Conditions
	EC:SG4.SP3 Manage Dependencies on Public Services
	EC:SG4.SP4 Manage Dependencies on Public Infrastructure
	EC:SG4.SP5 Plan for Facility Retirement

Specific Practices by Goal

EC:SG1 Establish and Prioritize Facility Assets

Facility assets are prioritized to ensure resilience of high-value services that they support.

EC:SG1.SP1 Prioritize Facility Assets

Facility assets are prioritized relative to their importance in supporting the delivery of high-value services.

EC:SG1.SP2 Establish Resilience-Focused Facility Assets

Facility assets that specifically support the organization's service continuity plans are identified and established.

EC:SG2 Protect Facility Assets

Administrative, technical, and physical controls for facility assets are identified, implemented, monitored, and managed.

EC:SG2.SP1 Assign Resilience Requirements to Facility Assets

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

EC:SG2.SP2 Establish and Implement Controls

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

EC:SG3 Manage Facility Asset Risk

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

EC:SG3.SP1 Identify and Assess Facility Asset Risk

Risks to facility assets are periodically identified and assessed.

EC:SG3.SP2 Mitigate Facility Risks

Risk mitigation strategies for facility assets are developed and implemented.

EC:SG4 Control Operational Environment

The operational environment of the facility is controlled to ensure its availability.

EC:SG4.SP1 Perform Facility Sustainability Planning

The availability of high-value facilities is ensured through sustainability planning.

EC:SG4.SP2 Maintain Environmental Conditions

Environmental conditions of the facility asset are maintained.

EC:SG4.SP3 Manage Dependencies on Public Services

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

EC:SG4.SP4 Manage Dependencies on Public Infrastructure

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

EC:SG4.SP5 Plan for Facility Retirement

The retirement of a facility is planned for to minimize operational impact.

ENTERPRISE FOCUS

Enterprise

Purpose

The purpose of Enterprise Focus is to establish sponsorship, strategic planning, and governance over the operational resilience management process.

Introductory Notes

Managing operational resilience requires a vast array of skills and competencies. These skills and competencies traverse the organization and must converge to achieve and sustain a desired level of operational resilience.

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

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

Enterprise Focus establishes the "critical few" for the organization—the high-value services that must be resilient to ensure mission achievement. This sets the focus for all operational risk-based activities in the organization. Through an enterprise focus, the direction and target for operational resilience management is established, operational risk management activities are coordinated, and actions are taken that enable the organization to perform adequately in achieving its targets.

Related Process Areas

Organizational risk drivers, risk appetite, and risk tolerance are established in the Risk Management process area.

The establishment of plans and programs to ensure service continuity is addressed in the Service Continuity process area.

The relationship between services and assets is addressed in Asset Definition and Management.

The management of compliance activities is addressed in the Compliance process area.

The development and achievement of resilience goals and objectives for staff is addressed in the Human Resource Management process area.

Providing awareness training for staff, both internal and external to the organization, is addressed in the Organizational Training and Awareness process area.

The Monitoring process area outlines processes for identifying, gathering, and communicating relevant data for decision making processes.

The establishment of resilience funding needs and the allocation of funds are addressed in the Financial Resource Management process area.

Summary of Specific Goals and Practices

Goals	Practices
EF:SG1 Establish Strategic Objectives	EF:SG1.SP1 Establish Strategic Objectives
	EF:SG1.SP2 Establish Critical Success Factors
	EF:SG1.SP3 Establish Organizational Services
EF:SG2 Plan for Operational Resilience	EF:SG2.SP1 Establish an Operational Resilience Management Plan
	EF:SG2.SP2 Establish an Operational Resilience Management Program
EF:SG3 Establish Sponsorship	EF:SG3.SP1 Commit Funding for Operational Resilience Management
	EF:SG3.SP2 Promote a Resilience-Aware Culture
	EF:SG3.SP3 Sponsor Resilience Standards and Policies
EF:SG4 Provide Resilience Oversight	EF:SG4.SP1 Establish Resilience as a Governance Focus Area
	EF:SG4.SP2 Perform Resilience Oversight
	EF:SG4.SP3 Establish Corrective Actions

Specific Practices by Goal

EF:SG1 Establish Strategic Objectives

The strategic objectives of the organization are established as the foundation for the operational resilience management process.

EF:SG1.SP1 Establish Strategic Objectives

Strategic objectives are identified and established as the basis for resilience activities.

EF:SG1.SP2 Establish Critical Success Factors

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

EF:SG1.SP3 Establish Organizational Services

The high-value services that support the accomplishment of strategic objectives are established.

EF:SG2 Plan for Operational Resilience

Planning for the operational resilience management process is performed.

EF:SG2.SP1 Establish an Operational Resilience Management Plan

A plan for managing operational resilience is established as the basis for the operational resilience management process.

EF:SG2.SP2 Establish an Operational Resilience Management Program

A program is established to carry out the activities and practices of the operational resilience management plan.

EF:SG3 Establish Sponsorship

Visible sponsorship of higher level managers for the operational resilience management process is established.

EF:SG3.SP1 Commit Funding for Operational Resilience Management

A commitment by higher level managers to fund resilience activities is established.

EF:SG3.SP2 Promote a Resilience Aware Culture

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

EF:SG3.SP3 Sponsor Resilience Standards and Policies

The development, implementation, enforcement, and management of resilience standards and policies are sponsored.

EF:SG4 Provide Resilience Oversight

Governance over the operational resilience management process is established and performed.

EF:SG4.SP1 Establish Resilience as a Governance Focus Area

Governance activities are extended to the operational resilience management process and accomplishment of the process goals.

EF:SG4.SP2 Perform Resilience Oversight

Oversight is performed over the operational resilience management process for adherence to established procedures, policies, standards, guidelines, and regulations.

EF:SG4.SP3 Establish Corrective Actions

Corrective actions are identified to address performance issues.

EXTERNAL DEPENDENCIES MANAGEMENT

Operations

Purpose

The purpose of External Dependencies Management is to establish and manage an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities.

Introductory Notes

Outsourcing services, development, production, and even asset management has become a normal and routine operational element for many organizations because it often provides the ability to engage specialist skills and equipment at a cost savings over internal equivalents. Increasingly, organizations are also exposing technology systems, information, and other high-value assets to customers to enable the seamless and efficient flow of business processes. The External Dependencies Management process area addresses the identification of risks associated with the actions of external entities, the formalization of the relationship with such entities, and the ongoing management of those dependencies and relationships, all in a manner to ensure that appropriate resilience measures are in place to protect and sustain the organization's services and assets that are dependent upon such actions and entities.

For the purpose of this process area, the term *organization* is used to refer to the entity—the enterprise or a part of the enterprise such as an organizational unit or department—that is using the process area. An external dependency exists when an entity that is external to the organization has access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization. Such entities may be contractors or customers, but they may also be other units or groups within the enterprise. In this process area, all such entities are referred to as *external entities*.

The success of the organization in accomplishing its overall mission depends on its ability to sustain mission assurance of services in a consistent and efficient manner. Some services are fully executed inside of organizational boundaries, giving the organization more direct control over mission assurance. However, in many cases, the organization does not control all of the activities in a service that contribute to meeting the service mission; instead, these activities may be performed by external entities.

Dependence on external entities may increase risk levels for organizations in managing the end-to-end resilience of their services. When the execution of a service extends outside of the organization's direct control, there is less ability to directly affect or predict mission assurance, in part because mission assurance is dependent on the resilience of the external entity. From an asset perspective—people, information, technology, and facilities—this can be problematic. In its role in support of a service, an external entity may

- use its own assets. If the external entity fails to protect and sustain these assets, the service and its outcome may be compromised.
- access the assets of the organization (which likely includes the ability to control or modify those assets). The external entity's actions could affect the resilience of the assets and thereby compromise the service.
- possess and use the assets of the organization (which includes the responsibility for custodial care of those assets). If the external entity fails to meet the resilience requirements of the assets (as specified by the organization), there is a potential impact on the service mission.
- develop, deliver, commission, or install a new or revised asset for the organization.
- provide supporting services that aid in protecting and sustaining an organization's asset.

Consider also that an external entity may not have a direct role in executing a specific service. In a support role (for example, storing information in an off-site storage facility), an external entity may also fail to adequately protect and sustain the asset such that it will not be available for use in a service when needed.

Regardless of the degree of external dependence, the organization retains responsibility for service mission assurance. The organization is responsible for setting the resilience requirements for services and related assets, communicating them to and requiring them of external entities, and monitoring to ensure external entities are meeting them. The evaluation and selection of external entities based on their abilities to sustain resilience is an important first step in ensuring service resilience.

External dependencies also arise when the organization outsources asset design or development activities—including facility development or software or systems development. *(Refer to the Resilient Technical Solutions Engineering process area for more information about developing systems and software in a manner that supports the organization's resilience requirements and program.)* Additional external dependencies arise when the organization is reliant on services that are part of the environment in which it operates, such as energy, telecommunications, and emergency response providers. All such external dependencies can significantly affect an organization's ability to achieve its service missions.

The External Dependencies Management process area comprises four goals: to identify and prioritize external dependencies, to manage risks associated with external dependencies, to formalize binding relationships with external entities, and to monitor and manage external entity performance against all contractual specifications including those for operational resilience.

Related Process Areas

The establishment and management of resilience requirements for the organization's assets, including those provided or controlled by external entities, are performed in the Resilience Requirements Development and the Resilience Requirements Management process areas.

The risk management cycle for external dependencies is addressed in the Risk Management process area.

The development, validation, testing, and improvement of plans to sustain service continuity for both the organization and external entities are addressed in the Service Continuity process area.

The availability of people to support the continued operation of services, including both employees of the organization and people provided by external entities, is addressed in the People Management process area.

Controls to manage the performance of people in support of the resilient operation of services, including both employees of the organization and people provided by external entities, is addressed in the Human Resource Management process area.

The identification, definition, management, and control of the organization's assets, including those provided or controlled by external entities, is addressed in the Asset Definition and Management process area.

The resilience of technology assets, including those in the control of the organization and those developed, provided, managed, or controlled by external entities, is addressed in the Technology Management process area.

The resilience of information assets, including those in the control of the organization and those provided, controlled, or accessed by external entities, is addressed in the Knowledge and Information Management process area.

The resilience of facility assets and control of the physical environment, including facilities in full control of the organization and those provided or managed by external entities, is addressed in the Environmental Controls process area.

The development of software and system assets that meet the organization's resilience requirements is addressed in the Resilient Technical Solution Engineering process area.

Summary of Specific Goals and Practices

Goals	Practices
EXD:SG1 Identify and Prioritize External Dependencies	EXD:SG1.SP1 Identify External Dependencies
	EXD:SG1.SP2 Prioritize External Dependencies
EXD:SG2 Manage Risks Due to External Dependencies	EXD:SG2.SP1 Identify and Assess Risks Due to External Dependencies
	EXD:SG2.SP2 Mitigate Risks Due to External Dependencies
EXD:SG3 Establish Formal Relationships	EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies
	EXD:SG3.SP2 Establish Resilience Specifications for External Dependencies
	EXD:SG3.SP3 Evaluate and Select External Entities
	EXD:SG3.SP4 Formalize Relationships
EXD:SG4 Manage External Entity Performance	EXD:SG4.SP1 Monitor External Entity Performance
	EXD:SG4.SP2 Correct External Entity Performance

EXD:SG1 Identify and Prioritize External Dependencies

External dependencies are identified and prioritized to ensure the resilience of the high-value services that they support.

EXD:SG1.SP1 Identify External Dependencies

Establish and maintain a list of external dependencies.

EXD:SG1.SP2 Prioritize External Dependencies

External dependencies are prioritized relative to their importance in supporting the delivery of high-value services.

EXD:SG2 Manage Risks Due to External Dependencies

Risks due to external dependencies are identified and managed.

EXD:SG2.SP1 Identify and Assess Risks Due to External Dependencies

Risks associated with external dependencies are periodically identified and assessed.

EXD:SG2.SP2 Mitigate Risks Due to External Dependencies

Risk mitigation strategies for external dependencies are developed and implemented.

EXD:SG3 Establish Formal Relationships

Relationships with external entities are formally established and maintained.

EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies

Enterprise specifications that apply in general to external entities are established and maintained.

EXD:SG3.SP2 Establish Resilience Specifications for External Dependencies

Resilience specifications that apply to specific external dependencies and entities are established and maintained.

EXD:SG3.SP3 Evaluate and Select External Entities

External entities are selected based on an evaluation of their ability to meet the specifications for external dependencies.

EXD:SG3.SP4 Formalize Relationships

Establish and maintain formal agreements with external entities.

EXD:SG4 Manage External Entity Performance

The performance of external entities is managed.

EXD:SG4.SP1 Monitor External Entity Performance

The performance of external entities is monitored against the specifications.

EXD:SG4.SP2 Correct External Entity Performance

Corrective actions are implemented to support external entity performance as necessary.

FINANCIAL RESOURCE MANAGEMENT

Enterprise

Purpose

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

Introductory Notes

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

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

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

Related Process Areas

Visible and active sponsorship and support for funding resilience activities is addressed in the Enterprise Focus process area.

The processes for identifying, analyzing, and mitigating risks that result from underfunding or lack of funding for resilience requirements are addressed in the Risk Management process area.

Summary of Specific Goals and Practices

Goals	Practices
FRM:SG1 Establish Financial Commitment	FRM:SG1.SP1 Commit Funding for Operational Resilience Management
	FRM:SG1.SP2 Establish Structure to Support Financial Management
FRM:SG2 Perform Financial Planning	FRM:SG2.SP1 Define Funding Needs
	FRM:SG2.SP2 Establish Resilience Budgets
	FRM:SG2.SP3 Resolve Funding Gaps
FRM:SG3 Fund Resilience Activities	FRM:SG3.SP1 Fund Resilience Activities
FRM:SG4 Account For Resilience Activities	FRM:SG4.SP1 Track and Document Costs
	FRM:SG4.SP2 Perform Cost And Performance Analysis
FRM:SG5 Optimize Resilience Expenditures and Investments	FRM:SG5.SP1 Optimize Resilience Expenditures
	FRM:SG5.SP2 Determine Return on Resilience Investments
	FRM:SG5.SP3 Identify Cost Recovery Opportunities

Specific Practices by Goal

FRM:SG1 Establish Financial Commitment

A commitment to funding resilience activities is established.

FRM:SG1.SP1 Commit Funding for Operational Resilience Management

A commitment by higher level managers to fund resilience activities is established.

FRM:SG1.SP2 Establish Structure to Support Financial Management

The structure that supports the assignment and management of financial resources to resilience activities is established.

FRM:SG2 Perform Financial Planning

Planning for funding resilience management activities is performed.

FRM:SG2.SP1 Define Funding Needs

The financial obligations for managing the operational resilience management process are established.

FRM:SG2.SP2 Establish Resilience Budgets

Capital and expense budgets for resilience management are established.

FRM:SG2.SP3 Resolve Funding Gaps

Identify and resolve gaps in funding for resilience management and mitigate associated risks.

FRM:SG3 Fund Resilience Activities

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

FRM:SG3.SP1 Fund Resilience Activities

Access to funds for resilience management activities is provided.

FRM:SG4 Account for Resilience Activities

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

FRM:SG4.SP1 Track and Document Costs

The costs associated with resilience management are tracked and documented.

FRM:SG4.SP2 Perform Cost and Performance Analysis

Cost and performance analysis for funded resilience management activities is performed.

FRM:SG5 Optimize Resilience Expenditures and Investments

The return to the organization for investment in resilience activities is measured and assessed.

FRM:SG5.SP1 Optimize Resilience Expenditures

Optimize the costs to implement and manage strategies to protect and sustain services and assets against the benefits.

FRM:SG5.SP2 Determine Return on Resilience Investments

Calculate a return on resilience investments where possible.

FRM:SG5.SP3 Identify Cost Recovery Opportunities

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

HUMAN RESOURCE MANAGEMENT

Enterprise

Purpose

The purpose of Human Resource Management is to manage the employment life cycle and performance of staff in a manner that contributes to the organization's ability to manage operational resilience.

Introductory Notes

The way that an organization hires, manages, and terminates staff can have a significant effect on the organization's operational resilience. The Human Resource Management competency seeks to address the management of staff in a way that minimizes operational risk and contributes to the organization's ability to manage operational resilience.

In Human Resource Management, the organization consciously approaches the acquisition of staff as an activity that can improve operational resilience by ensuring the acquisition of necessary skill sets and the avoidance of introducing operational risk that results from poor hiring decisions. Staff is acquired with a view toward their contributions to meeting the organization's mission with an understanding and acceptance of their role in sustaining operational resilience. This helps staff to begin acculturation to the organization's philosophy on operational resilience as they become part of the organization.

The management of staff performance is a means by which the organization can enforce (and reinforce) its philosophy on operational resilience. In Human Resource Management, the organization reinforces the connection between staff and operational resilience by using the performance management program as a way to acculturate staff to their resilience roles and responsibilities. Job descriptions include these roles and responsibilities, which are enforced by the organization by their inclusion in annual goal setting. The organization specifically establishes acceptable performance behaviors and measures compliance with these behaviors on a regular basis as part of the performance management cycle. As a result, the organization inculcates a resilience-aware and ready culture that is essential for supporting the resilience process and the organizational mission.

Human Resource Management also seeks to ensure that the organization's human resources do not pose additional operational risk to the organization when they voluntarily or involuntarily sever their employment. Changes in employment can have significant effects on operational resilience by potentially disrupting the contributions of staff to the productive capacity of services. In addition, because staff typically have other organizational assets in their possession, when they vacate their positions the repossession of these assets by the organization may be critical to operational resilience, particularly if sensitive information assets or technology assets are not returned. Finally, involuntary separations may be disruptive—they can affect services and the morale and motivation of existing staff. Thus, the organization must act in a way that minimizes the impact of involuntary terminations and limits unpredictable effects on productive capacity.

The Human Resource Management competency covers the employment life cycle—hiring, performance management, and termination. It has four specific goals addressing the

identification of skill requirements, the acquisition of appropriate staff, the management of staff performance in supporting operational resilience, and the termination of staff in a manner that minimizes organizational impact.

As people are a ubiquitous resource to an organization, there are many aspects of human resources that affect operational resilience. People Management is focused on the availability of people to the services that they support. The management of people through their employment life cycle and the effect on operational resilience is addressed in the Human Resource Management competency. Finally, promoting awareness of the organization's efforts and providing training to resilience staff for their roles in managing operational resilience is addressed in the Organizational Training and Awareness competency.

Related Process Areas

The training of staff to meet resilience requirements, needs, and gaps is established and managed in the Organizational Training and Awareness process area.

Determining funding needs for providing human resources to the operational resilience management process is addressed in the Financial Resource Management process area.

The management of operational risks through their life cycle is addressed in the Risk Management process area.

The specific activities involved in cross-training and succession planning as a means for improving and sustaining resilience is addressed in the People Management process area.

The management of intellectual property and knowledge as high-value organizational information assets is addressed in the Knowledge and Information Management process area.

Managing access to organizational assets on a recurring basis is addressed in the Access Management process area.

Summary of Specific Goals and Practices

Goals	**Practices**
HRM:SG1 Establish Resource Needs	HRM:SG1.SP1 Establish Baseline Competencies
	HRM:SG1.SP2 Inventory Skills and Identify Gaps
	HRM:SG1.SP3 Address Skill Deficiencies
HRM:SG2 Manage Staff Acquisition	HRM:SG2.SP1 Verify Suitability of Candidate Staff
	HRM:SG2.SP2 Establish Terms and Conditions of Employment
HRM:SG3 Manage Staff Performance	HRM:SG3.SP1 Establish Resilience as a Job Responsibility
	HRM:SG3.SP2 Establish Resilience Performance Goals and Objectives
	HRM:SG3.SP3 Measure and Assess Performance
	HRM:SG3.SP4 Establish Disciplinary Process
HRM:SG4 Manage Changes to Employment Status	HRM:SG4.SP1 Manage Impact of Position Changes
	HRM:SG4.SP2 Manage Access to Assets
	HRM:SG4.SP3 Manage Involuntary Terminations

HRM:SG1 Establish Resource Needs

The resource needs to staff the activities and tasks of the organization's resilience program and plan are identified and satisfied.

HRM:SG1.SP1 Establish Baseline Competencies

The staffing and skill needs relative to the operational resilience management process are established.

HRM:SG1.SP2 Inventory Skills and Identify Gaps

The current skill set for operational resilience management is inventoried and gaps in necessary skills are identified.

HRM:SG1.SP3 Address Skill Deficiencies

Gaps in skills necessary to meet operational resilience management needs are addressed.

HRM:SG2 Manage Staff Acquisition

The acquisition of staff to meet operational needs is performed with consideration of the organization's resilience objectives.

HRM:SG2.SP1 Verify Suitability of Candidate Staff

Candidate staff are evaluated for suitability against position requirements and risks.

HRM:SG2.SP2 Establish Terms and Conditions of Employment

Employment agreements appropriate for the position and role are developed and executed.

HRM:SG3 Manage Staff Performance

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

HRM:SG3.SP1 Establish Resilience as a Job Responsibility

Resilience obligations for staff are communicated, agreed to, and documented as conditions of employment.

HRM:SG3.SP2 Establish Resilience Performance Goals and Objectives

Goals and objectives for supporting the organization's resilience program are established as part of the performance management process.

HRM:SG3.SP3 Measure and Assess Performance

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

HRM:SG3.SP4 Establish Disciplinary Process

A disciplinary process is established for staff who violate resilience policies.

HRM:SG4 Manage Changes to Employment Status

Changes in the employment status of staff members in the organization are managed.

HRM:SG4.SP1 Manage Impact of Position Changes

Administrative controls are established to sustain functions, obligations, and vital roles upon position changes or terminations.

HRM:SG4.SP2 Manage Access to Assets

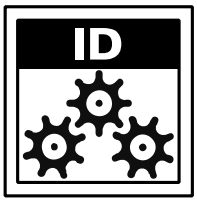
Access to and possession of organizational assets relative to position changes is managed.

HRM:SG4.SP3 Manage Involuntary Terminations

Administrative controls and procedures are established to manage the effects of involuntary terminations.

IDENTITY MANAGEMENT

Operations



Purpose

The purpose of Identity Management is to create, maintain, and deactivate identities that may need some level of trusted access to organizational assets and to manage their associated attributes.

Introductory Notes

Identity management is a process that addresses the life cycle of identities for objects and entities (systems, devices, or other processes) and for persons that need some level of trusted access to organizational assets (information; systems, servers, and networks; and facilities).

In identity management, identities for persons, objects, and entities are created so that they are made known to the organization and can be managed throughout their useful life. In the case of persons, these identities typically represent users of information, systems, and facilities who have unique identifying names (such as a user ID) and for whom information is known about their job roles and responsibilities in the organization. The creation of an identity is a means for profiling the person, object, or entity such that the identity retains a particular set of specific information (often referred to as the identity's DNA) as it traverses the organization and is provided different levels of trusted access to diverse organizational assets. This concept may even extend beyond the organization's borders. For example, a particular person, object, or entity may have more than one identity across different organizations that can be accumulated into a single identity (through a process called federation).

The importance of establishing identities and understanding their DNA is so that they can be assigned access to organizational assets (through a process called provisioning) and so that this access can be managed as the operational environment changes. This is tremendously important to managing operational resilience in that unauthorized or unintended access to organizational assets may result in unwanted outcomes such as

- disclosure of information (resulting in violations of privacy and confidentiality requirements)
- unauthorized use of systems and servers (to carry out fraudulent activities)
- unauthorized entry to secured facilities (which could affect the life, safety, and health of staff and customers)
- destruction or loss of vital information and systems that the organization relies upon day-to-day to carry out its strategic objectives

Because the operating environment is complex and the persons, objects, and entities which need access to organizational assets are ever-changing, the organization must actively manage the population of identities to ensure that it is valid. This is a challenging task that requires coordination and cooperation between the areas of the organization where identities

are created and managed (for example, in the IT department) and other departments such as human resources (where changes to the community of users are detected) and legal (where new business partners and vendors may have contractual agreements that require access or ownership of assets).

Roles and responsibilities are linked to an organizational identity; that is, what a person or object has responsibility for in the organization (their role) determines the type and extent of access that is provided. Some roles are trusted—extraordinary access to organizational access is provided as a necessity for performing a distinct (and sometimes unique) job function. The role is associated with specific access privileges and restrictions that are imposed on the identity when access is provisioned.

Identities must be deprovisioned—that is, when the person, object, or entity ceases to exist in the organization, the identity is eliminated and by reference all of its access privileges and restrictions are eliminated as well. The failure to deprovision an identity can result in significant operational risk to an organization because it may provide an identity to which an unauthorized (and perhaps unknown) person, object, or entity can associate. If this occurs and requisite access privileges have not been terminated, the identity can be stolen and provided by default with all of the existing privileges.

Identity management is often seen as a technical construct. This is because many of the processes for managing identities are operationalized as software packages and focus on electronic access to intangible assets such as information or to technical assets such as software, systems, hardware, and networks. However, in a broad sense, identity management is about establishing the existence of a person, object, or entity in the organization to which one or more access privileges can be assigned. These privileges can be electronic or physical (such as when providing access privileges to technology and facility assets). In some cases, identities may be established without any access privileges being provided.

To properly manage organizational identities, the organization must have processes to establish identities, deprovision identities, and manage changes that occur in the population of identities based on changes in the operating environment. Identities must be described in sufficient detail so that their attributes, including their roles and responsibilities, are clear and can be used as the basis for determining the appropriateness of assigning access privileges and restrictions.

Identity management and the management of access privileges are tightly coupled but distinct activities. An identity must exist to describe a particular role or responsibility in the organization. Access privileges are provided to the identity by virtue of its role. While connected, each of these activities represents a distinct aspect of access control and management that must be mastered to ensure that only authorized staff have access to organizational assets based on their need.

Related Process Areas

Access control and management is addressed in the Access Management process area.

Risks related to inconsistencies between identities and the persons, objects, and entities they represent are addressed in the Risk Management process area.

Summary of Specific Goals and Practices

Goals	Practices
ID:SG1 Establish Identities	ID:SG1.SP1 Create Identities
	ID:SG1.SP2 Establish Identity Community
	ID:SG1.SP3 Assign Roles to Identities
ID:SG2 Manage Identities	ID:SG2.SP1 Monitor and Manage Identity Changes
	ID:SG2.SP2 Periodically Review and Maintain Identities
	ID:SG2.SP3 Correct Inconsistencies
	ID:SG2.SP4 Deprovision Identities

Specific Practices by Goal

ID:SG1 Establish Identities

Identities are created to represent persons, objects, and entities that require access to organizational assets.

ID:SG1.SP1 Create Identities

Persons, objects, and entities that require access to organizational assets are registered and profiled.

ID:SG1.SP2 Establish Identity Community

The identity community is established and documented.

ID:SG1.SP3 Assign Roles to Identities

Organizational roles are established and associated with identities.

ID:SG2 Manage Identities

Identities are managed to ensure they reflect the current environment of associated persons, objects, and entities.

ID:SG2.SP1 Monitor and Manage Identity Changes

Changes to identities are monitored for and managed.

ID:SG2.SP2 Periodically Review and Maintain Identities

Periodic review is performed to identify identities that are invalid.

ID:SG2.SP3 Correct Inconsistencies

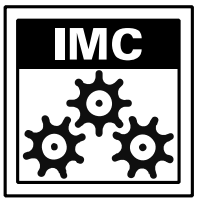
Inconsistencies between the identity community and the persons, objects, and entities they represent are corrected.

ID:SG2.SP4 Deprovision Identities

Deprovision identities for which need has expired or has been eliminated.

INCIDENT MANAGEMENT AND CONTROL

Operations



Purpose

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

Introductory Notes

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

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

The Incident Management and Control process area focuses the organization's attention on the life cycle of an incident—from event detection to analysis to response. The organization establishes the incident management plan and program and assigns appropriate resources. Event detection and reporting capabilities are established, and the organization sets criteria to establish when events become incidents that demand its attention. Events are triaged and analyzed, and incidents are validated. Supporting activities such as communication, logging and tracking events and incidents, and preserving event and incident evidence are defined and established. Most importantly, the organization performs post-incident review to determine what can be learned from incident management and applied to improve strategies for protecting and sustaining services and assets, as well as improvements in the incident management process and life cycle.

Incident management begins with event identification, triage, and analysis. An event can be one or more minor occurrences that affect organizational assets and have the potential to disrupt operations. An event may not require a formal response from the organization—it may be an isolated issue or problem that is immediately or imminently fixable and does not pose organizational harm. For example, a user may report that they have opened an email attachment and now their workstation is not operating properly. This "event" may be an isolated problem or an operator error that requires attention but may not require an organizational response.

Other events (or series of events) require the organization to take notice. Upon triage and analysis, these events may be declared as "incidents" by the organization. An incident is an event (or series of events) of higher magnitude that significantly affects organizational assets

and associated services and requires the organization to respond in some way to prevent or limit organizational impact. For example, several customers may independently report that they are unable to place orders via the internet (events). The problem is deemed to be caused by a denial-of-service attack that is being targeted against the web portal (incident). In this case, the organization must be able to recognize, analyze, and manage the incident successfully. When an organization is dealing with an incident whose impact to the organization is rapidly escalating or immediate, the incident is deemed a "crisis." A crisis requires immediate organizational action because the effect of the incident is already being felt by the organization and must be limited or contained.

Incidents affect the productivity of the organization's assets and, in turn, associated services. Because assets span physical and electronic forms, incidents can be either cyber or physical in nature, depending on the target of the incident. Incidents that affect the people and facilities assets are typically physical in nature. In the case of information and technology assets, incidents can be cyber (such as unauthorized access to electronic information or to technology components) or physical (such as unauthorized access to paper or other media on which information assets are stored or to technology assets that are physically accessible).

Operational resilience is predicated on the organization's ability to identify disruptive events, prevent them where possible, and respond to them when the organization is impacted. The extent to which the organization performs event management must be commensurate with the desired level of operational resilience that it needs to achieve its mission.

Incident management is a broad organizational function. It includes many types of activities that traverse the enterprise and require varying skill sets. To provide effective coverage of these activities, the Incident Management and Control process area has five goals that address

- incident planning and assignment of resources
- event and incident identification and reporting
- event analysis
- incident response and recovery
- incident learning and knowledge management

Related Process Areas

Developing, testing, and implementing service continuity plans is addressed in the Service Continuity process area.

Reporting incidents according to applicable laws, rules, and regulations is addressed in the Compliance process area.

The processes for identifying and detecting events that could become incidents are addressed in the Monitoring process area.

Managing risks to organizational assets that arise from incidents is addressed in the Risk Management process area.

Summary of Specific Goals and Practices

Goals	Practices
IMC:SG1 Establish the Incident Management and Control Process	IMC:SG1.SP1 Plan for Incident Management
	IMC:SG1.SP2 Assign Staff to the Incident Management Plan
IMC:SG2 Detect Events	IMC:SG2.SP1 Detect and Report Events
	IMC:SG2.SP2 Log and Track Events
	IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence
	IMC:SG2.SP4 Analyze and Triage Events
IMC:SG3 Declare Incidents	IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria
	IMC:SG3.SP2 Analyze Incidents
IMC:SG4 Respond to and Recover from Incidents	IMC:SG4.SP1 Escalate Incidents
	IMC:SG4.SP2 Develop Incident Response
	IMC:SG4.SP3 Communicate Incidents
	IMC:SG4.SP4 Close Incidents
IMC:SG5 Establish Incident Learning	IMC:SG5.SP1 Perform Post-Incident Review
	IMC:SG5.SP2 Integrate with the Problem Management Process
	IMC:SG5.SP3 Translate Experience to Strategy

Specific Practices by Goal

IMC:SG1 Establish the Incident Management and Control Process

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

IMC:SG1.SP1 Plan for Incident Management

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

IMC:SG1.SP2 Assign Staff to the Incident Management Plan

Staff are identified and assigned to the incident management plan.

IMC:SG2 Detect Events

Establish and maintain a process for detecting, reporting, triaging, and analyzing events.

IMC:SG2.SP1 Detect and Report Events

Events are detected and reported.

IMC:SG2.SP2 Log and Track Events

Events are logged and tracked from inception to disposition.

IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence

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

IMC:SG2.SP4 Analyze and Triage Events

Events are analyzed and triaged to support event resolution and incident declaration.

IMC:SG3 Declare Incidents

Incidents are declared and analyzed to support response planning.

IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria

Criteria for declaring incidents is defined and maintained.

IMC:SG3.SP2 Analyze Incidents

Analyze incidents to support the development of an appropriate incident response.

IMC:SG4 Respond to and Recover from Incidents

The process for responding to and recovering from incidents is established.

IMC:SG4.SP1 Escalate Incidents

Incidents are escalated to the appropriate stakeholders for input and resolution.

IMC:SG4.SP2 Develop Incident Response

A response to a declared incident is developed and implemented to prevent or limit organizational impact.

IMC:SG4.SP3 Communicate Incidents

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

IMC:SG4.SP4 Close Incidents

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

IMC:SG5 Establish Incident Learning

Lessons learned from identifying, analyzing, and responding to incidents are translated into actions to improve strategies for protecting and sustaining services and assets.

IMC:SG5.SP1 Perform Post-Incident Review

Post-incident review is performed to determine underlying causes.

IMC:SG5.SP2 Integrate with the Problem Management Process

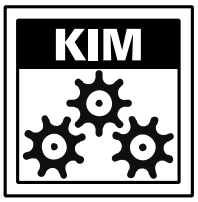
A link between incident handling and the organization's problem management process is established.

IMC:SG5.SP3 Translate Experience to Strategy

The lessons learned from incident management are analyzed and translated into service and asset protection and continuity strategies.

KNOWLEDGE AND INFORMATION MANAGEMENT

Operations



Purpose

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

Introductory Notes

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

An information asset can be described as information or data that is of value to the organization, including such diverse information as patient records, intellectual property, vital business records and contracts, and customer information. The unique aspect of information assets is that they can exist in physical form (on paper, CDs, or other media) or electronic form (files, databases, on personal computers). The Knowledge and Information Management process area addresses the importance of information assets in the operational resilience of services, as well as unique attributes specific to information assets such as those described in Table 1.

Table 1: Attributes of Information Assets

availability	For an information asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed.
confidentiality	For an information asset, the quality of being accessible only to authorized people, processes, and devices.
integrity	For an information asset, the quality of being in the condition intended by the owner and so continuing to be useful for the purposes intended by the owner.
privacy	The assurance that information about an individual is disclosed only to people, processes, and devices authorized by that individual or permitted under privacy laws and regulations.
sensitivity	A measure of the degree to which an information asset must be protected based on the consequences of its unauthorized access, modification, or disclosure.

In this process area, information assets are prioritized according to their value in supporting high-value organizational services. Physical, technical, and administrative controls that keep information assets viable and sustainable are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, information asset risks are identified and mitigated in an attempt to prevent disruption where possible. Information is categorized as to its organizational sensitivity, and considerations are made for the backup and storage of important information and vital records in case of loss or destruction, or to support the execution of service continuity plans.

Knowledge management is also performed in this process area: the requirement to identify and document the organizational and intellectual knowledge of staff that is important to the effective operation of the organization's services. This information asset is often not documented, has poorly developed security requirements, and lacks adequate protection. It is also often one of the most high-value information assets in the organization.

Related Process Areas

The establishment and management of resilience requirements for information assets is performed in the Resilience Requirements Development and Resilience Requirements Management process areas.

The identification, definition, inventorying, management, and control of information assets is addressed in the Asset Definition and Management process area.

The risk management cycle for information assets is addressed in the Risk Management process area.

The management of the internal control system that ensures the protection of information assets is addressed in the Controls Management process area.

The selection, implementation, and management of access controls for information assets is performed in the Access Management and Control process area.

Summary of Specific Goals and Practices

Goals	Practices
KIM:SG1 Establish and Prioritize Information Assets	KIM:SG1.SP1 Prioritize Information Assets
	KIM:SG1.SP2 Categorize Information Assets
KIM:SG2 Protect Information Assets	KIM:SG2.SP1 Assign Resilience Requirements to Information Assets
	KIM:SG2.SP2 Establish and Implement Controls
KIM:SG3 Manage Information Asset Risk	KIM:SG3.SP1 Identify and Assess Information Asset Risk
	KIM:SG3.SP2 Mitigate Information Asset Risk
KIM:SG4 Manage Information Asset Confidentiality and Privacy	KIM:SG4.SP1 Encrypt High-Value Information
	KIM:SG4.SP2 Control Access to Information Assets
	KIM:SG4.SP3 Control Information Asset Disposition
KIM:SG5 Manage Information Asset Integrity	KIM:SG5.SP1 Control Modification to Information Assets
	KIM:SG5.SP2 Manage Information Asset Configuration
	KIM:SG5.SP3 Verify Validity of Information
KIM:SG6 Manage Information Asset Availability	KIM:SG6.SP1 Perform Information Duplication and Retention
	KIM:SG6.SP2 Manage Organizational Knowledge

KIM:SG1 Establish and Prioritize Information Assets

Information assets are prioritized to ensure the resilience of high-value services in which they are used.

KIM:SG1.SP1 Prioritize Information Assets

Information assets are prioritized relative to their importance in supporting the delivery of high-value services.

KIM:SG1.SP2 Categorize Information Assets

Information assets that support high-value services are categorized as to their organizational sensitivity.

KIM:SG2 Protect Information Assets

Administrative, technical, and physical controls for information assets are identified, implemented, monitored, and managed.

KIM:SG2.SP1 Assign Resilience Requirements to Information Assets

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

KIM:SG2.SP2 Establish and Implement Controls

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

KIM:SG3 Manage Information Asset Risk

Operational risks to information assets are identified and managed.

KIM:SG3.SP1 Identify and Assess Information Asset Risk

Risks to information assets are periodically identified and assessed.

KIM:SG3.SP2 Mitigate Information Asset Risk

Risk mitigation strategies for information assets are developed and implemented.

KIM:SG4 Manage Information Asset Confidentiality and Privacy

The confidentiality and privacy considerations of information assets are managed.

KIM:SG4.SP1 Encrypt High-Value Information

Cryptographic controls are applied to information assets to ensure confidentiality and prevent accidental disclosure.

KIM:SG4.SP2 Control Access to Information Assets

Access controls are developed and implemented to limit access to information assets.

KIM:SG4.SP3 Control Information Asset Disposition

The means for disposing of information assets is controlled.

KIM:SG5 Manage Information Asset Integrity

The integrity of information assets to support high-value services is managed.

KIM:SG5.SP1 Control Modification to Information Assets

The modification of information assets is controlled.

KIM:SG5.SP2 Manage Information Asset Configuration

Information asset baselines are created and changes are managed.

KIM:SG5.SP3 Verify Validity of Information

Controls are implemented to sustain the validity and reliability of information assets.

KIM:SG6 Manage Information Asset Availability

The availability of information assets to support high-value services is managed.

KIM:SG6.SP1 Perform Information Duplication and Retention

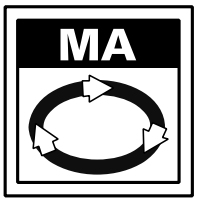
High-value information assets are backed up and retained to support services when needed.

KIM:SG6.SP2 Manage Organizational Knowledge

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

MEASUREMENT AND ANALYSIS

Process



Purpose

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

Introductory Notes

Consistent, timely, and accurate measurements are important feedback for managing any activity. Measurement and Analysis represents a means for applying metrics, measurement, and analysis to the resilience equation. This process area represents the organization's application of measurement as a foundational activity to provide data and analysis results that can be effectively used to inform and improve the management of the resilience process.

In the Measurement and Analysis process area, the organization establishes the objectives for measurement (i.e., what it intends to accomplish) and determines the measures that would be useful to managing the operational resilience management process as well as to provide meaningful data to management for the processes of governance, compliance, monitoring, and improvement. The organization collects relevant data, analyzes this data, and provides reports to managers and other stakeholders to support decision making.

In a generic sense, the measurement and analysis process includes the following activities and objectives:

- specifying the objectives of measurement and analysis such that they are aligned with identified information needs and objectives
- specifying the measures, analysis techniques, and mechanism for data collection, data storage, reporting, and feedback
- implementing the collection, storage, analysis, and reporting of the data
- providing objective results that can be used in making informed decisions, and taking appropriate corrective actions

Integrating measurement and analysis into the operational resilience management process supports

- planning, estimating, and executing operational resilience management activities
- tracking the performance of operational resilience management activities against established plans and objectives, including resilience requirements
- identifying and resolving issues in the operational resilience management processes
- providing a basis for incorporating measurement into additional operational resilience management processes in the future

Measurement and analysis activities are often most effective when focused at the organizational unit or line of business level. Since operational resilience management is an enterprise-wide concern, however, it's important for the enterprise to have mechanisms in place to make use of that local data at the enterprise level, particularly as the enterprise matures. Repositories for measurement data at the organizational unit or line of business level will be purposeful for local optimization, but as data is shared across organizational units for the overall improvement benefit of the enterprise, measurement repositories may also be needed at the enterprise level.

Related Process Areas

Measurement and analysis needs are informed by the organization's governance activities, which are addressed in the Enterprise Focus process area.

Some of the data specified for Measurement and Analysis may be gathered and distributed through processes described in the Monitoring process area.

Measurements may be necessary as evidence of compliance; compliance requirements are addressed in the Compliance process area.

Summary of Specific Goals and Practices

Goals	Practices
MA:SG1 Align Measurement and Analysis Activities	MA:SG1.SP1 Establish Measurement Objectives
	MA:SG1.SP2 Specify Measures
	MA:SG1.SP3 Specify Data Collection and Storage Procedures
	MA:SG1.SP4 Specify Analysis Procedures
MA:SG2 Provide Measurement Results	MA:SG2.SP1 Collect Measurement Data
	MA:SG2.SP2 Analyze Measurement Data
	MA:SG2.SP3 Store Data and Results
	MA:SG2.SP4 Communicate Results

Specific Practices by Goal

MA:SG1 Align Measurement and Analysis Activities

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

MA:SG1.SP1 Establish Measurement Objectives

Measurement objectives are established and maintained based on information needs and objectives.

MA:SG1.SP2 Specify Measures

The measures necessary to meet measurement objectives are established.

MA:SG1.SP3 Specify Data Collection and Storage Procedures

The techniques for collecting and storing measurement data are specified.

MA:SG1.SP4 Specify Analysis Procedures

The techniques for analysis and reporting are specified.

MA:SG2 Provide Measurement Results

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

MA:SG2.SP1 Collect Measurement Data

Measurement data is collected consistent with measurement objectives.

MA:SG2.SP2 Analyze Measurement Data

Measurement data are analyzed against measurement objectives.

MA:SG2.SP3 Store Data and Results

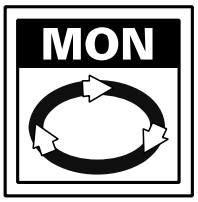
Measurement data, analysis, and results are stored.

MA:SG2.SP4 Communicate Results

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

MONITORING

Process



Purpose

The purpose of Monitoring is to collect, record, and distribute information about the operational resilience management process to the organization on a timely basis.

Introductory Notes

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

Many operational resilience management processes implicitly require monitoring capacities in order to achieve higher-maturity goals. For example, monitoring provides data about changes in the user environment that can result in necessary changes in access privileges. Effective monitoring also informs the organization when new vulnerabilities emerge (either inside or outside of the organization) or when events or incidents require the organization's attention. This information may require the organization to change its strategy, improve control selection, implementation, and management, or improve the details of its service continuity plans. In addition, the organization's compliance process—which is by nature data-intensive—benefits from monitoring activities by receiving up-to-date information that can be important to compliance activities. In essence, monitoring is a core capability that the organization must master in order to improve and sustain a level of adequate resilience.

Monitoring is also a data collection activity that allows the organization to measure process effectiveness across resilience capabilities. For example, through monitoring, the organization can determine whether its resilience goals are being met. It can also ascertain whether its security activities are effective and producing the intended results. Monitoring is one way that the organization collects necessary data (and invokes a vital feedback loop) to know how well it is performing in managing the operational resilience management process.

The Monitoring process area focuses on the activities the organization performs to collect, record, and distribute relevant data to the organization for the purposes of managing resilience and providing data for measuring process effectiveness. To do this, the organization must establish the stakeholders of the monitoring process (i.e., those who have a need for timely information about resilience activities) and determine their requirements and needs. The organization must also determine its monitoring requirements for managing both operational resilience and the operational resilience management process and ensure that resources have been assigned to meet these requirements. Data collection, recording, and distribution takes organizational resources, thus, the organization must consider and implement an infrastructure that

supports and enables its monitoring needs and capabilities. Finally, the organization must collect, organize, record, and make available the necessary information in a manner that is timely and accurate and that ensures data confidentiality, integrity, and availability.

Related Process Areas

The Monitoring process area provides essential data necessary to manage several operational resilience management processes. These processes include Incident Management and Control, Vulnerability Assessment and Resolution, Risk Management, and others. From a process improvement perspective, all operational resilience management process areas may rely upon data collected and distributed through monitoring practices as described in this process area.

Summary of Specific Goals and Practices

Goals	Practices
MON:SG1 Establish and Maintain a Monitoring Program	MON:SG1.SP1 Establish Monitoring Program
	MON:SG1.SP2 Identify Stakeholders
	MON:SG1.SP3 Establish Monitoring Requirements
	MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements
MON:SG2 Perform Monitoring	MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure
	MON:SG2.SP2 Establish Collection Standards and Guidelines
	MON:SG2.SP3 Collect and Record Information
	MON:SG2.SP4 Distribute Information

Specific Practices by Goal

MON:SG1 Establish and Maintain a Monitoring Program

Establish and maintain a program for identifying, recording, collecting, and reporting important resilience information.

MON:SG1.SP1 Establish Monitoring Program

Establish and maintain the program for identifying, collecting, and distributing monitoring information.

MON:SG1.SP2 Identify Stakeholders

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

MON:SG1.SP3 Establish Monitoring Requirements

The requirements for monitoring operational resilience management processes are established.

MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements

Monitoring requirements are analyzed and prioritized to ensure they can be satisfied.

MON:SG2 Perform Monitoring

The monitoring process is performed throughout the enterprise.

MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure

A monitoring infrastructure commensurate with meeting monitoring requirements is established and maintained.

MON:SG2.SP2 Establish Collection Standards and Guidelines

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

MON:SG2.SP3 Collect and Record Information

Information relevant to the operational resilience management process is collected and recorded.

MON:SG2.SP4 Distribute Information

Collected and recorded information is distributed to appropriate stakeholders.

ORGANIZATIONAL PROCESS DEFINITION

Process

Purpose

The purpose of Organizational Process Definition (OPD) is to establish and maintain a usable set of organizational process assets and work environment standards for operational resilience.

Introductory Notes

Organizational process assets enable consistent resilience management process performance across the organization and provide a basis for cumulative, long-term benefits to the organization. *(See the definition of "organizational process assets" in the glossary.)*

The organization's process asset library is a collection of items maintained by the organization for use by the people and organizational units of the organization. This collection of items includes descriptions of processes and process elements, descriptions of life-cycle models, process tailoring guidelines, process-related documentation, and data. The organization's process asset library supports organizational learning and process improvement by allowing the sharing of best practices and lessons learned across the organization.

The organization's set of standard processes is tailored by organizational units to create their defined processes. The other organizational process assets are used to support tailoring and the implementation of the defined processes. The work environment standards are used to guide creation of organizational unit work environments.

A standard process is composed of other processes (i.e., subprocesses) or process elements. A process element is the fundamental (e.g., atomic) unit of process definition and describes the activities and tasks to consistently perform work. Process architecture provides rules for connecting the process elements of a standard process. The organization's set of standard processes may include multiple process architectures.

(See the definitions of "standard process," "process architecture," "subprocess," and "process element" in the glossary.)

The organizational process assets may be organized in many ways, depending on the implementation of the Organizational Process Definition process area. Examples include the following:

- The organization's set of standard processes may be stored in the organization's process asset library, or they may be stored separately.
- A single repository may contain both the measurements and the process-related documentation, or they may be stored separately.

Related Process Areas

Refer to the Organizational Process Focus process area for more information about organizational process related matters.

Summary of Specific Goals and Practices

Goals	Practices
OPD:SG1 Establish Organizational Process Assets	OPD:SG1.SP1 Establish Standard Processes
	OPD:SG1.SP2 Establish Tailoring Criteria and Guidelines
	OPD:SG1.SP3 Establish the Organization's Measurement Repository
	OPD:SG1.SP4 Establish the Organization's Process Asset Library
	OPD:SG1.SP5 Establish Work Environment Standards
	OPD:SG1.SP6 Establish Rules and Guidelines for Integrated Teams

Specific Practices by Goal

OPD:SG1 Establish Organizational Process Assets

A set of organizational process assets is established and maintained.

OPD:SG1.SP1 Establish Standard Processes

The organization's set of standard processes are established and maintained.

OPD:SG1.SP2 Establish Tailoring Criteria and Guidelines

Tailoring criteria and guidelines for the organization's set of standard processes are established and maintained.

OPD:SG1.SP3 Establish the Organization's Measurement Repository

The organization's measurement repository is established and maintained.

OPD:SG1.SP4 Establish the Organization's Process Asset Library

The organization's process asset library is established and maintained.

OPD:SG1.SP5 Establish Work Environment Standards

Work environment standards are established and maintained.

OPD:SG1.SP6 Establish Rules and Guidelines for Integrated Teams

Organizational rules and guidelines for the structure, formation, and operation of integrated teams are established and maintained.

ORGANIZATIONAL PROCESS FOCUS

Process

Purpose

The purpose of Organizational Process Focus (OPF) is to plan, implement, and deploy organizational process improvements based on a thorough understanding of current strengths and weaknesses of the organization's operational resilience processes and process assets.

Introductory Notes

The organization's processes include all operational resilience processes used by the organization and its organizational units. Candidate improvements to the organization's processes and process assets are obtained from various sources, including the measurement of processes, lessons learned in implementing processes, results of process appraisals, results of post-event or incident handling, results of customer satisfaction evaluation, results of benchmarking against other organizations' processes, and recommendations from other improvement initiatives in the organization.

Process improvement occurs in the context of the organization's needs and is used to address the organization's objectives. The organization encourages participation in process improvement activities by those who perform the process. The responsibility for facilitating and managing the organization's process improvement activities, including coordinating the participation of others, is typically assigned to an operational resilience process group. The organization provides the long-term commitment and resources required to sponsor this group and to ensure the effective and timely deployment of improvements.

Careful planning is required to ensure that process improvement efforts across the organization are adequately managed and implemented. Results of the organization's process improvement planning are documented in a process improvement plan.

The "organization's process improvement plan" addresses appraisal planning, process action planning, pilot planning, and deployment planning. Appraisal plans describe the appraisal timeline and schedule, the scope of the appraisal, resources required to perform the appraisal, the reference model against which the appraisal will be performed, and logistics for the appraisal.

Process action plans usually result from appraisals and document how improvements targeting weaknesses uncovered by an appraisal will be implemented. Sometimes the improvement described in the process action plan should be tested on a small group before deploying it across the organization. In these cases, a pilot plan is generated.

When the improvement is to be deployed, a deployment plan is created. This plan describes when and how the improvement will be deployed across the organization.

Organizational process assets are used to describe, implement, and improve the organization's processes. *(See the definition of "organizational process assets" in the glossary.)*

Related Process Areas

Refer to the Organizational Process Definition process area for more information about establishing organizational process assets, including standard processes.

Summary of Specific Goals and Practices

Goals	Practices
OPF:SG1 Determine Process Improvement Opportunities	OPF:SG1.SP1 Establish Organizational Process Needs
	OPF:SG1.SP2 Appraise the Organization's Processes
	OPF:SG1.SP3 Identify the Organization's Process Improvements
OPF:SG2 Plan and Implement Process Actions	OPF:SG2.SP1 Establish Process Action Plans
	OPF:SG2.SP2 Implement Process Action Plans
OPF:SG3 Deploy Organizational Process Assets and Incorporate Experiences	OPF:SG3.SP1 Deploy Organizational Process Assets
	OPF:SG3.SP2 Deploy Standard Processes
	OPF:SG3.SP3 Monitor the Implementation
	OPF:SG3.SP4 Incorporate Experiences into Organizational Process Assets

Specific Practices by Goal

OPF:SG1 Determine Process Improvement Opportunities

Strengths, weaknesses, and improvement opportunities for the organization's processes are identified periodically and as needed.

OPF:SG1.SP1 Establish Organizational Process Needs

The description of process needs and objectives for the organization are established and maintained.

OPF:SG1.SP2 Appraise the Organization's Processes

The organization's processes are appraised periodically and as needed to maintain an understanding of their strengths and weaknesses.

OPF:SG1.SP3 Identify the Organization's Process Improvements

Improvements to the organization's processes and process assets are identified.

OPF:SG2 Plan and Implement Process Actions

Process actions that address improvements to the organization's processes and process assets are planned and implemented.

OPF:SG2.SP1 Establish Process Action Plans

Process action plans to address improvements to the organization's processes and process assets are established and maintained.

OPF:SG2.SP2 Implement Process Action Plans

Process action plans are implemented.

OPF:SG3 Deploy Organizational Process Assets and Incorporate Experiences

Organizational process assets are deployed across the organization and process-related experiences are incorporated into organizational process assets.

OPF:SG3.SP1 Deploy Organizational Process Assets

Organizational process assets are deployed across the organization.

OPF:SG3.SP2 Deploy Standard Processes

Deploy the organization's set of standard processes to organizational units (including projects at their startup) and deploy changes to them as appropriate.

OPF:SG3.SP3 Monitor the Implementation

The organization's set of standard processes and use of process assets is monitored.

OPF:SG3.SP4 Incorporate Experiences into Organizational Process Assets

Process-related work products, measures, and improvement information derived from planning and performing the process are incorporated into organizational process assets.

ORGANIZATIONAL TRAINING AND AWARENESS

Enterprise

Purpose

The purpose of Organizational Training and Awareness is to promote awareness and develop skills and knowledge of people in support of their roles in attaining and sustaining operational resilience.

Introductory Notes

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

Organizational Training and Awareness focuses exclusively on skills, knowledge, and cognizance for resilience activities, not generalized training across the organization. However, these resilience training and awareness activities should integrate with and be supported by the organization's overall training and awareness program and plan. Specifically, training refers to imparting the necessary skills and knowledge to people for performing their roles and responsibilities in support of the organization's operational resilience management process. Awareness is aimed at focusing the attention of staff throughout the organization on resilience issues, concerns, policies, plans, and practices, and increasing their cognizance of and acculturation to resilience. Training imparts skills and knowledge to enable staff to perform a specific resilience function; awareness activities create cognizance to bring about desired behaviors in support of the resilience process and to support a risk-aware culture in the organization.

An organizational training and awareness program is a comprehensive capability that typically includes the following activities:

- identifying the training and awareness needs of the organization
- sourcing training and awareness materials
- providing training and implementing awareness activities, using a variety of methods
- establishing and maintaining records of training and awareness activities
- evaluating the effectiveness of the training and awareness program
- revising the program to improve effectiveness and in response to changes in training and awareness needs

The Organizational Training and Awareness process area has four specific goals. The Establish Awareness Program goal addresses the creation, planning, and organization of an

awareness program. Conduct Awareness Activities puts awareness plans into action throughout the enterprise and evaluates their effectiveness. The Establish Training goal addresses the creation, planning, and organization of a training capability. Conduct Training addresses the delivery and evaluation of training activities.

Organizational Training and Awareness is a complementary process area to the Human Resource Management and People Management process areas. Organizational Training and Awareness focuses on general awareness, skill-building, and ongoing training. Human Resource Management is focused on managing the employment life cycle and performance for an employee in support of operational resilience. People Management identifies key staff and manages their availability to the services they support, ensuring the resilience of the "people" asset.

Related Process Areas

Managing the resilience of the people in the organization is performed in the People Management process area.

Managing the employment life cycle and performance for an employee in support of operational resilience is addressed in the Human Resource Management process area.

Awareness activities for third parties such as business partners and vendors are addressed in the External Dependencies Management process area.

Awareness communications are addressed in the Communications process area.

Tracking awareness activities for compliance purposes is addressed in the Compliance process area.

Guidance about tracking awareness activities for governance functions is addressed in the Enterprise Focus process area.

Summary of Specific Goals and Practices

Goals	Practices
OTA:SG1 Establish Awareness Program	OTA:SG1.SP1 Establish Awareness Needs
	OTA:SG1.SP2 Establish Awareness Training Plan
	OTA:SG1.SP3 Establish Awareness Training Capability
OTA:SG2 Conduct Awareness Activities	OTA:SG2.SP1 Perform Awareness Activities
	OTA:SG2.SP2 Establish Awareness Records
	OTA:SG2.SP3 Assess Awareness Program Effectiveness
OTA:SG3 Establish Training Capability	OTA:SG3.SP1 Establish Training Needs
	OTA:SG3.SP2 Establish Training Plan
	OTA:SG3.SP3 Establish Training Capability
OTA:SG4 Conduct Training	OTA:SG4.SP1 Deliver Training
	OTA:SG4.SP2 Establish Training Records
	OTA:SG4.SP3 Assess Training Effectiveness

OTA:SG1 Establish Awareness Program

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

OTA:SG1.SP1 Establish Awareness Needs

The awareness needs of the organization are established and maintained.

OTA:SG1.SP2 Establish Awareness Plan

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

OTA:SG1.SP3 Establish Awareness Delivery Capability

A capability for consistent and repeatable delivery of awareness artifacts is established and maintained.

OTA:SG2 Conduct Awareness Activities

Awareness activities that support the organization's resilience program are performed.

OTA:SG2.SP1 Perform Awareness Activities

Awareness activities are performed according to the awareness plan.

OTA:SG2.SP2 Establish Awareness Records

Records of awareness activities performed are established and maintained.

OTA:SG2.SP3 Assess Awareness Program Effectiveness

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

OTA:SG3 Establish Training Capability

Training capabilities that support the operational resilience management process are established and maintained.

OTA:SG3.SP1 Establish Training Needs

The training needs of the organization are established and maintained.

OTA:SG3.SP2 Establish Training Plan

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

OTA:SG3.SP3 Establish Training Capability

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

OTA:SG4 Conduct Training

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

OTA:SG4.SP1 Deliver Resilience Training

Training is delivered according to the training plan.

OTA:SG4.SP2 Establish Training Records

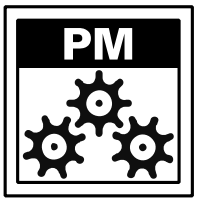
Records of delivered training are established and maintained.

OTA:SG4.SP3 Assess Training Effectiveness

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

PEOPLE MANAGEMENT

Operations



Purpose

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

Introductory Notes

People are an essential asset in the organization's ability to produce products and deliver services in the pursuit of strategic objectives. Without people and their skills, knowledge, information, and other valuable traits, many business processes could not operate effectively and the mission of organizational services would be in jeopardy.

The People Management process area focuses specifically on the "people" asset and their role in supporting the operation of business processes and services. Unlike information, technology, and facilities, the primary resilience requirement for people is availability—the availability of people to perform their roles and responsibilities in supporting organizational services as intended and when necessary. Events that disrupt the contributions of people affect the successful outcome of business processes and services and may impede the organization's mission. Even in highly automated operating environments where people have diminished roles, the unavailability of people may render services unable to meet their missions.

To properly manage people and their contributions to services, the organization must address several key aspects of resilience. It must

- identify the vital people in the organization, based on their roles and responsibilities
- identify and manage risks that would interrupt or disrupt the contributions of people or make people unavailable to perform their roles and responsibilities
- manage the processes that ensure continued availability of people or that provide for appropriate substitutions and replacements when necessary
- manage the availability of people during and after disruptive events and other times of stress

While there is an assumption that people who support organizational services are typically employed directly by the organization, there are many cases where they are acquired through outsourcing and supplier relationships or may be otherwise external to the organization. These external staff are included in the scope of the People Management process area because their availability could affect the successful operation of business processes and services. Therefore, the "staff" referred to in this process area can be understood to include both internal and external parties. In addition, the availability of people also extends to staff who are deployed in vital resilience roles in disciplines such as security, business continuity and disaster recovery, first response, and IT operations management.

The People Management process area considers the effects on the organization due to interruptions and disruptions that affect the performance and availability of people. Thus, considerations such as cross-training of staff and succession planning are included to ensure

a steady stream of effective staff for vital job roles and responsibilities. In addition, the impact of staff turnover, particularly in vital roles in high-value services, is also considered and addressed. When disruptions occur, People Management focuses the organization on preparing staff to accept and perform new roles, however temporary, until a return to business as usual can be accomplished. This can be a challenge because of physiological and physical constraints that the organization may have to identify and address before staff can effectively be re-introduced to a post-event workplace environment. All of these potential issues must be acknowledged and addressed by the organization in order to ensure sustained productivity of people throughout the enterprise.

As people are a ubiquitous resource to an organization, there are many aspects of people that affect operational resilience. People Management is focused on the availability of people to the services that they support. The management of people through their employment life cycle and the effect on operational resilience is addressed in the Human Resource Management process area. Finally, promoting awareness of the organization's efforts and providing training to resilience staff for their roles in managing operational resilience is addressed in the Organizational Training and Awareness process area.

Related Process Areas

The establishment and management of resilience requirements for people are performed in the Resilience Requirements Definition and Resilience Requirements Management process areas.

The identification of people and their support for services is addressed in the Asset Definition and Management process area.

The risk management cycle for people is addressed in the Risk Management process area.

The management of the internal control system that ensures people are adequately protected is addressed in the Controls Management process area.

The role of people in sustaining high-value organizational services and business processes is addressed in the Service Continuity process area.

The management of the human resources life cycle (from hiring to termination) is addressed in the Human Resource Management process area.

The awareness and acculturation of staff to the organization's philosophy and approach to managing operational resilience is addressed in the Organizational Training and Awareness process area.

Summary of Specific Goals and Practices

Goals	Practices
PM:SG1 Establish Vital Staff	PM:SG1.SP1 Identify Vital Staff
PM:SG2 Manage Risks Associated with Staff Availability	PM:SG2.SP1 Identify and Assess Staff Risk
	PM:SG2.SP2 Mitigate Staff Risk
PM:SG3 Manage the Availability of Staff	PM:SG3.SP1 Establish Redundancy for Vital Staff
	PM:SG3.SP2 Perform Succession Planning
	PM:SG3.SP3 Prepare for Redeployment
	PM:SG3.SP4 Plan to Support Staff During Disruptive Events
	PM:SG3.SP5 Plan for Return-to-Work Considerations

PM:SG1 Establish Vital Staff

The vital staff of the organization are identified and prioritized.

PM:SG1.SP1 Identify Vital Staff

The vital staff from a resilience perspective are identified and characterized.

PM:SG2 Manage Risks Associated with Staff Availability

Operational risks related to the availability of staff are identified and managed.

PM:SG2.SP1 Identify and Assess Staff Risk

Risks to the availability of staff are periodically identified and assessed.

PM:SG2.SP2 Mitigate Staff Risk

Mitigation strategies for the risks related to the availability of staff are developed and implemented.

PM:SG3 Manage the Availability of Staff

The availability of staff to support high-value services is managed.

PM:SG3.SP1 Establish Redundancy for Vital Staff

Redundancy for vital staff is established to ensure continuity of services.

PM:SG3.SP2 Perform Succession Planning

Vital management roles and responsibilities are supported through succession planning.

PM:SG3.SP3 Prepare for Redeployment

Establish plans and prepare staff for redeployment to other roles during a disruptive event or in the execution of a continuity of operations plan.

PM:SG3.SP4 Plan to Support Staff During Disruptive Events

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

PM:SG3.SP5 Plan for Return-to-Work Considerations

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

RISK MANAGEMENT

Enterprise

Purpose

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

Introductory Notes

Risk management is a basic and essential organizational capability. The organization must identify, analyze, and mitigate risk commensurate with its risk tolerances and appetite to ensure that it prevents potential disruptions that could interfere with its ability to meet its mission. At a tactical level, to accomplish this goal the organization must control operational risk—the risk that results from operating services and associated assets on a day-to-day basis. Operational risk encompasses the potential impact that could result from

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

Managing operational risk significantly influences operational resilience. The risk of disruption to any asset potentially renders associated services unable to meet their mission, hence reducing operational resilience. The organization must identify this risk, analyze it, and determine the extent to which it could affect operations. Mitigating such risk requires a careful balance between strategies for protecting and sustaining assets and services while considering the cost of these strategies and the value of the asset and service to the organization.

The Risk Management process area establishes the organization's responsibility to develop and implement an operational risk management plan and program that comprehensively and cooperatively covers the high-value assets and services of the organization. The organization explicitly establishes its risk tolerances and appetite based on its strategic drivers, market position, competitive environment, financial position, and other factors. Using this appetite as a guide, risks to the assets of the organization are periodically identified, analyzed, and categorized, and mitigation strategies are developed and implemented for those risks that the organization cannot afford to ignore. The impact of risk is considered and measured against the organization's risk evaluation criteria. Most importantly, the information gathered in risk assessment can be used to improve the effectiveness of strategies to protect and sustain assets and services.

All uses of "risk" in Risk Management refer to operational risk, specifically, risk to the operation and delivery of services. Other risk categories are beyond the scope of this process area.

Related Process Areas

The identification of vulnerabilities that may pose risk to the organization is performed in the Vulnerability Analysis and Resolution process area.

The development and implementation of control strategies to mitigate risk is performed in the Controls Management process area.

The development, testing, and implementation of service continuity plans to address the consequences of realized risk is performed in the Service Continuity process area.

Summary of Specific Goals and Practices

Goals	Practices
RISK:SG1 Prepare for Risk Management	RISK:SG1.SP1 Determine Risk Sources and Categories
	RISK:SG1.SP2 Establish an Operational Risk Management Strategy
RISK:SG2 Establish Risk Parameters and Focus	RISK:SG2.SP1 Define Risk Parameters
	RISK:SG2.SP2 Establish Risk Measurement Criteria
RISK:SG3 Identify Risk	RISK:SG3.SP1 Identify Asset-Level Risks
	RISK:SG3.SP2 Identify Service-Level Risks
RISK:SG4 Analyze Risk	RISK:SG4.SP1 Evaluate Risk
	RISK:SG4.SP2 Categorize and Prioritize Risk
	RISK:SG4.SP3 Assign Risk Disposition
RISK:SG5 Mitigate and Control Risk	RISK:SG5.SP1 Develop Risk Mitigation Plans
	RISK:SG5.SP2 Implement Risk Strategies
RISK:SG6 Use Risk Information to Manage Resilience	RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services
	RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services

Specific Practices by Goal

RISK:SG1 Prepare for Risk Management

Preparation for risk management is performed.

RISK:SG1.SP1 Determine Risk Sources and Categories

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

RISK:SG1.SP2 Establish an Operational Risk Management Strategy

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

RISK:SG2 Establish Risk Parameters and Focus

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

RISK:SG2.SP1 Define Risk Parameters

The organization's risk parameters are defined.

RISK:SG2.SP2 Establish Risk Measurement Criteria

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

RISK:SG3 Identify Risk

Operational risks are identified.

RISK:SG3.SP1 Identify Asset-Level Risks

Operational risks that affect assets that support services are identified.

RISK:SG3.SP2 Identify Service-Level Risks

Operational risks that potentially affect services as a result of asset risk are identified.

RISK:SG4 Analyze Risk

Risks are analyzed to determine priority and importance.

RISK:SG4.SP1 Evaluate Risk

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

RISK:SG4.SP2 Categorize and Prioritize Risk

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

RISK:SG4.SP3 Assign Risk Disposition

The disposition of each identified risk is documented and approved.

RISK:SG5 Mitigate and Control Risk

Risks to assets and services are mitigated and controlled to prevent disruption of operational resilience.

RISK:SG5.SP1 Develop Risk Mitigation Plans

Risk mitigation plans are developed.

RISK:SG5.SP2 Implement Risk Strategies

Risk strategies and mitigation plans are implemented and monitored.

RISK:SG6 Use Risk Information to Manage Resilience

Information gathered from identifying, analyzing, and mitigating risk is used to improve the operational resilience management process.

RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services

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

RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services

Service continuity plans are developed to ensure services are sustained and plans are evaluated and updated as required based on risk information.

RESILIENCE REQUIREMENTS DEVELOPMENT

Engineering

Purpose

The purpose of Resilience Requirements Development is to identify, document, and analyze the operational resilience requirements for high-value services and related assets.

Introductory Notes

An operational resilience requirement is a constraint that the organization places on the productive capability of a high-value asset to ensure that it remains viable and can be sustained when charged into production to support a high-value service. In practice, operational resilience requirements are a derivation of the traditionally described security objectives of confidentiality, integrity, and availability. Well known as descriptive properties or quality attributes of information assets, these objectives are also extensible to other types of assets—people, technology, and facilities—with which operational resilience management is concerned.

Resilience requirements provide the foundation for protecting assets from threats and sustaining them to the extent practical and possible so that they can perform as intended in support of services. In essence, resilience requirements become a part of an asset's DNA (just like its definition, owner, and value) that transcends departmental and organizational boundaries because they stay with the asset regardless of where it is deployed or operated.

Requirements drive engineering-based processes, such as operational resilience management. In the operational resilience management process, the Resilience Requirements Development process area requires the organization to establish resilience requirements at the enterprise, service, and asset levels. Resilience requirements also drive or influence many of the process areas in the definition of the operational resilience management process. For example, resilience requirements form the basis for developing controls and strategies for protecting assets (Controls Management) and for developing service continuity plans for services and assets (Service Continuity).

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

Depending on the organization, three types of operational resilience requirements may be elicited: enterprise, service, and asset.

- **Enterprise**. Enterprise operational resilience requirements reflect enterprise-level needs, expectations, and constraints. These requirements affect nearly all aspects of an organization's operations. Laws and regulations are examples of this type of requirement because they broadly affect the business in which an organization operates and must be met by all organizational functions and activities. A specific example of an enterprise

requirement is “all health-related information that is covered by HIPAA regulations must be kept confidential to health workers and patients.”

- **Service**. Service requirements establish the resilience needs of a service in pursuit of its mission. But because the capability of a service to meet its mission is directly related to the resilience of the assets that support the service, service requirements must reflect and be congruent with the operational resilience requirements of supporting assets. Service requirements tend to concentrate on the service’s availability and recoverability, but these quality attributes can be directly affected by failure to meet the confidentiality, integrity, and availability requirements of people, information, technology, and facilities.
- **Asset**. Asset-specific requirements are set by the owners of the asset and are intended to establish the needs for protecting and sustaining an asset with respect to its role in supporting mission assurance of a service. In practice, asset-specific resilience requirements generally reflect the security objectives of confidentiality and integrity and the continuity requirement of availability. It must be considered that assets also may have conflicting requirements, particularly where they are deployed in supporting more than one service (e.g., a network server may support more than service). This conflict must be resolved to ensure that all services that are dependent on the asset are provided the necessary level of resilience to meet their mission.

The applicability of a specific type of resilience requirement varies depending on the asset type, as shown in Table 1.

Table 1: Extension of resilience requirements to all types of resilience assets

Resilience Requirement	**Asset Type**			
	People	**Information**	**Technology**	**Facilities**
Confidentiality	--	x	--	--
Integrity	--	x	x	x
Availability	x	x	x	x

There are many ways in which an organization can elicit resilience requirements. Strategic planning efforts may establish enterprise-level requirements, as would direct interviewing of vital organizational managers. Service-level requirements may be established by owners of the service (e.g., an organizational unit or a line of business). Asset-level requirements may be established through regular security risk assessment and business impact analysis activities and through directly interviewing the owners of the assets, who understand their importance to services and are responsible for their productivity and resilience.

All resilience requirements must be analyzed for conflicts and interdependencies and must be validated against and support the accomplishment of enterprise-level organizational drivers (goals, objectives, and critical success factors). Otherwise, the protection and continuity strategies developed and implemented for assets and services will not align with what the organization needs to accomplish in order to remain viable.

The development of resilience requirements typically includes the following activities:

- identifying organizational drivers and preparing these work products so that they can be used as the foundation for setting resilience requirements
- developing and communicating enterprise-level requirements
- developing and communicating service and asset-level requirements

- regularly analyzing the requirements to ensure alignment with current organizational drivers, to identify conflict between enterprise and asset-level requirements, and to satisfy operational constraints
- validating the requirements against organizational drivers and operational constraints

The Resilience Requirements Development process area has three specific goals:

1. The Identify Enterprise Requirements goal addresses the development of enterprise-level requirements that potentially affect all services and assets.
2. The Develop Service Requirements goal addresses the development of service-level requirements through the identification of asset requirements and the assignment of enterprise requirements to services.
3. The Analyze and Validate Requirements goal addresses the analysis of service-level requirements to ensure that they support strategic drivers and the resolution of conflicting requirements.

The goals of the Resilience Requirements Development process area are supported and managed long term by achievement of the goals in the Resilience Requirements Management process area.

Related Process Areas

The identification of high-value assets and the assignment of resilience requirements to assets and services are performed in the Asset Definition and Management process area.

The identification of high-value services is performed in the Enterprise Focus process area.

The identification and prioritization of risks to high-value services and supporting assets is performed in the Risk Management process area.

Resilience requirements are managed in the Resilience Requirements Management process area.

Summary of Specific Goals and Practices

Goals	Practices
RRD:SG1 Identify Enterprise Requirements	RRD:SG1.SP1 Establish Enterprise Resilience Requirements
RRD:SG2 Develop Service Requirements	RRD:SG2.SP1 Establish Asset Resilience Requirements
	RRD:SG2.SP2 Assign Enterprise Resilience Requirements to Services
RRD:SG3 Analyze and Validate Requirements	RRD:SG3.SP1 Establish a Definition of Required Functionality
	RRD:SG3.SP2 Analyze Resilience Requirements
	RRD:SG3.SP3 Validate Resilience Requirements

RRD:SG1 Identify Enterprise Requirements

The organization's enterprise-level resilience requirements are identified and established.

RRD:SG1.SP1 Establish Enterprise Resilience Requirements

The resilience requirements of the enterprise are established.

RRD:SG2 Develop Service Requirements

The resilience requirements for services are developed and established based on the service mission and the requirements of supporting assets.

RRD:SG2.SP1 Establish Asset Resilience Requirements

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

RRD:SG2.SP2 Assign Enterprise Resilience Requirements to Services

Enterprise requirements that affect services are assigned to the services.

RRD:SG3 Analyze and Validate Requirements

The resilience requirements for services are analyzed and validated.

RRD:SG3.SP1 Establish a Definition of Required Functionality

Establish and maintain a definition of the required functionality of assets in the context of the services they support.

RRD:SG3.SP2 Analyze Resilience Requirements

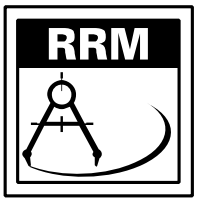
Analyze the requirements of assets to identify conflicts, interdependencies, and shared requirements.

RRD:SG3.SP3 Validate Resilience Requirements

Ensure that the asset-level resilience requirements adequately specify what is needed to protect and sustain an asset commensurate with its value.

RESILIENCE REQUIREMENTS MANAGEMENT

Engineering



Purpose

The purpose of Resilience Requirements Management is to manage the resilience requirements of high-value services and associated assets and to identify inconsistencies between these requirements and the activities that the organization performs to meet the requirements.

Introductory Notes

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

The Resilience Requirements Management process area aims to ensure that the requirements that are established in the Resilience Requirements Development process area (or are otherwise acquired) remain viable for each high-value asset associated with a high-value service until it is retired (either because the asset is retired or its relative value is reduced) or until it is changed due to one or more organizational triggers. In addition, Resilience Requirements Management defines the organization's responsibility for monitoring the effectiveness of requirements (for protecting service-related assets and ensuring their continuity) and for recognizing when changes to requirements are necessary. Finally, the evolution of requirements often necessitates that an organization revisit the goals and practices in the Resilience Requirements Development process area because organizational drivers must be re-established, new or revised enterprise-level or asset-level requirements must be developed, or changes to requirements must be analyzed and revalidated. The iterative nature of the Resilience Requirements Development and Resilience Requirements Management process areas is necessary to ensure that asset-level resilience requirements satisfactorily reflect and support strategic drivers, which in turn supports the level of operational resilience that the organization desires.

The Resilience Requirements Management process area has one specific goal—to manage resilience requirements. In practice, this requires that the organization obtain and promote an understanding of the requirements, ensure commitment to satisfying the requirements, manage changes to the requirements, establish traceability of the requirements, and identify inconsistencies between the requirements and the activities that the organization performs to satisfy them.

Related Process Areas

The identification, development, documentation, and analysis of resilience requirements is performed in the Resilience Requirements Development process area.

The responsibility for managing requirements at the asset level is established in the Asset Definition and Management process area.

Ensuring that requirements reflect the protection and continuity needs of the owners of the assets is performed in the Resilience Requirements Development process area.

Identifying and establishing the ownership of the assets and the corresponding responsibilities for establishing and validating resilience requirements is performed in the Asset Definition and Management process area.

The monitoring and control of the satisfaction of resilience requirements for high-value business processes, services, and associated assets is performed in the Monitoring process area.

Summary of Specific Goals and Practices)

Goals	Practices
RRM:SG1 Manage Requirements	RRM:SG1.SP1 Obtain an Understanding of Resilience Requirements
	RRM:SG1.SP2 Obtain Commitment to Resilience Requirements
	RRM:SG1.SP3 Manage Resilience Requirements Changes
	RRM:SG1.SP4 Maintain Traceability of Resilience Requirements
	RRM:SG1.SP5 Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements

Specific Practices by Goal

RRM:SG1 Manage Requirements

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

RRM:SG1.SP1 Obtain an Understanding of Resilience Requirements

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

RRM:SG1.SP2 Obtain Commitment to Resilience Requirements

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

RRM:SG1.SP3 Manage Resilience Requirements Changes

Changes to resilience requirements are managed as conditions dictate.

RRM:SG1.SP4 Maintain Traceability of Resilience Requirements

Traceability between resilience requirements and the activities performed to satisfy the requirements is established.

RRM:SG1.SP5 Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements

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

RESILIENT TECHNICAL SOLUTION ENGINEERING

Engineering

Purpose

The purpose of Resilient Technical Solution Engineering is to ensure that software and systems are developed to satisfy their resilience requirements.

Introductory Notes

Software and systems are pervasive organizational assets that automate services and support business processes to help organizations meet their missions. The importance of resilient technical solutions—software and systems that resist threats, function satisfactorily in the face of adversity, and continue to help services meet their missions under times of stress—cannot be overstated.

Resilient software and systems do not become survivable and resistant to threat without an organizational commitment to address resilience throughout the development process. These assets must be specifically designed and developed with consideration of the types of threats they will face, the operating conditions and changing risk environment in which they will operate, and the priority and needs to sustain the services they support. Typical software and systems development life cycles understandably focus on identifying and satisfying functional requirements; that is, most of the effort goes into defining and designing what the software or system must do to fulfill its use case, purpose, objectives, and ultimately, its mission. However, requirements for quality attributes such as security, availability, performance, reliability, and the ability to sustain software and system assets can in the long run be equally important to the usability and longevity of software and system assets and require considerable resources to address in the operations phase if they are not considered early in the development life cycle.

Unfortunately, quality attribute requirements can be harder to define, design, and implement, and in many cases require significant business impact and cost analysis up front to ensure that they are worth investing in. This leads to a tendency to ignore these requirements early in the development life cycle and to bolt on solutions to address them later in the design and implementation phases, when they are more costly, less effective, and typically harder to manage and sustain in an operational mode. The failure to consider requirements for quality attributes is a primary reason why software and systems in operation are subjected to high levels of operational risk resulting from failed technology and processes. This expands an already complex operational risk environment brought about by the integration of software and systems with other technology assets such as information, hardware, networks, and telecommunications. In essence, ignoring quality attributes creates additional security, continuity, and other related operational risks that must be managed in the operations phase of the life cycle, typically at higher cost, lower efficacy, and potentially increased consequences to the organization. In some cases, these problems may be so significant as to shorten the expected life of the software and systems, diminish their overall operational resilience, and result in cumulatively lower than expected return on investment.

The functional aspects of software and systems do not have meaning if they are not resistant to disruption or cannot be sustained under degraded conditions. High-quality software and systems cannot be produced and sustained without addressing these issues early in the development life cycle. The controls necessary to demonstrate that integrity and availability requirements are met must be identified as early as the needs determination phase. Controls can then be designed to fit the architecture and functionality of the software and systems in their expected operating environment and can be implemented and made operable to ensure that they achieve the desired effect. This process cannot be shortchanged; it must be wholly integrated into the organization's development process and must be measured, managed, and improved in the same manner as highly effective and mature software and systems development processes.

Developing or acquiring resilient technical solutions such as software and systems requires a dedicated process that encompasses the asset's life cycle. The process begins by establishing a plan for addressing resilience as part of the organization's regular development life cycle and the integration of the plan into the organization's corresponding development process. The identification, development, and validation of quality attribute requirements are performed alongside similar processes for functional requirements. Resilient software and systems are designed through the elicitation and identification of resilience requirements and the design of architectures that reflect a resilience focus, including security, operations controls, and the ability to sustain software and system assets. Resilient software and systems are developed through processes that include secure coding of software, software defect detection and removal, and the development of resilience controls based on design specifications. The resilience controls for software and systems are tested, and issues are referred back to the design and development cycle for resolution. Reviews are conducted throughout the development life cycle to ensure that resilience is kept in the forefront and given adequate attention and consideration. System-specific continuity planning is performed and integrated with service continuity planning to ensure that software, systems, hardware, networks, telecommunications, and other technical assets can be sustained. A post-implementation review of deployed systems is performed to ensure that resilience requirements are being satisfied as intended.

In operations, software and systems are monitored to determine if there is variability that could indicate the effects of threats or vulnerabilities and to ensure that controls are functioning properly. Configuration management and change control processes are implemented to ensure software and systems are kept up to date to address newly discovered vulnerabilities and weaknesses (particularly in vendor-acquired products and components) and to prevent the intentional or inadvertent introduction of malicious code or other exploitable vulnerabilities.

To effectively integrate resilience considerations, the organization must establish guidelines for developing resilient software and systems, develop a plan for selecting, tailoring, and integrating selected guidelines into existing development life cycles and processes for any given development project, and then execute the plan. Plan development and execution includes identifying and mitigating risks to the success of the development project.

The Resilient Technical Solution Engineering process area is strongly influenced by two Capability Maturity Model Integration (CMMI) process areas [CMMI Product Team 2006]:

- Requirements Development, the purpose of which is to produce and analyze customer requirements and software and system product and product component requirements.

- Technical Solution, the purpose of which is to design, develop, and implement solutions to software and system requirements. Solutions, designs, and implementations encompass software and system products, product components, and product-related life-cycle processes, either singly or in combination as appropriate.

There are a growing number of reputable sources to consider when identifying and selecting candidate guidelines for the development of resilient software and systems across the life cycle, particularly for software security and assurance.

These are examples of sources of guidelines:

- Building Security In Maturity Model (BSIMM2) v2.0
  http://www.bsi-mm.com/
- Open Web Applications Security Project (OWASP) Software Assurance Maturity Model (SAMM) v1.0
  http://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model
- Microsoft's Security Development Life Cycle, Version 4.1
  http://www.microsoft.com/security/sdl/
- Department of Homeland Security Assurance for CMMI Process Reference Model
  https://buildsecurityin.us-cert.gov/swa/procwg.html

The Resilient Technical Solution Engineering process area assumes that the organization has one or more existing, defined processes for software and system development into which resilience controls and activities can be integrated. If this is not the case, the organization should not attempt to implement the goals and practices identified in this process area.

Note: This process area does not address the unique aspects of the resilience of embedded systems or the resilience of hardware that is part of a software-intensive system.

Related Process Areas

Resilience requirements for software and system technology assets in operation, including those that may influence quality attribute requirements in the development process, are developed and managed in the Resilience Requirements Development and Resilience Requirements Management process areas respectively.

Identifying and adding newly developed and acquired software and system assets to the organization's asset inventory is addressed in the Asset Definition and Management process area.

The management of resilience for technology assets as a whole, particularly for deployed, operational assets, is addressed in the Technology Management process area. This includes, for example, asset fail-over, backup, recovery, and restoration.

Acquiring software and systems from external entities and ensuring that such assets meet their resilience requirements throughout the asset life cycle is addressed in the External Dependencies Management process area. That said, RTSE specific goals and practices should be used to aid in evaluating and selecting external entities that are developing software and systems (EXD:SG3.SP3), formalizing relationships with such external entities (EXD:SG3.SP4), and managing an external entity's performance when developing software and systems (EXD:SG4).

Monitoring for events, incidents, and vulnerabilities that may affect software and systems in operation is addressed in the Monitoring process area.

Service continuity plans are identified and created in the Service Continuity process area. These plans may be inclusive of software and systems that support the services for which planning is performed.

Summary of Specific Goals and Practices)

Goals	Practices
RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development	RTSE:SG1.SP1 Identify General Guidelines
	RTSE:SG1.SP2 Identify Requirements Guidelines
	RTSE:SG1.SP3 Identify Architecture and Design Guidelines
	RTSE:SG1.SP4 Identify Implementation Guidelines
	RTSE:SG1.SP5 Identify Assembly and Integration Guidelines
RTSE:SG2 Develop Resilient Technical Solution Development Plans	RTSE:SG2.SP1 Select and Tailor Guidelines
	RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process
RTSE:SG3 Execute the Plan	RTSE:SG3.SP1 Monitor Execution of the Development Plan
	RTSE:SG3.SP2 Release Resilient Technical Solutions into Production

Specific Practices by Goal

RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development

Guidelines are developed to ensure proper consideration of resilience activities and controls in all phases of the life cycle.

RTSE:SG1.SP1 Identify General Guidelines

General guidelines for building resilience into software and systems are identified.

RTSE:SG1.SP2 Identify Requirements Guidelines

Guidelines for determining software and systems resilience requirements are identified.

RTSE:SG1.SP3 Identify Architecture and Design Guidelines

Guidelines for designing resilience into software and systems are identified.

RTSE:SG1.SP4 Identify Implementation Guidelines

Guidelines for implementing resilient software and systems are identified.

RTSE:SG1.SP5 Identify Assembly and Integration Guidelines

Guidelines for the assembly and integration of resilient software into resilient systems are identified.

RTSE:SG2 Develop Resilient Technical Solution Development Plans

Plans for addressing resilience in the development life cycle are based on documented guidelines.

RTSE:SG2.SP1 Select and Tailor Guidelines

Guidelines are determined for a specific software or system development project using selection criteria.

RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process

Selected resilience guidelines are integrated with a defined software and systems development process and a documented plan.

RTSE:SG3 Execute the Plan

Progress against the plan for developing resilient software and systems is monitored throughout the development life cycle.

RTSE:SG3.SP1 Monitor Execution of the Development Plan

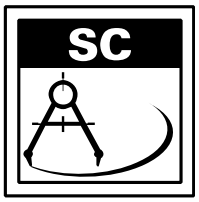
Execution of the development plan is monitored to ensure that software and system resilience requirements are satisfied.

RTSE:SG3.SP2 Release Resilient Technical Solutions into Production

Software and systems that demonstrate satisfaction of resilience requirements are released into production.

SERVICE CONTINUITY

Engineering



Purpose

The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

Introductory Notes

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

Service Continuity describes the organizational processes responsible for developing, deploying, exercising, implementing, and managing plans for responding to and recovering from events and restoring operations to business as usual. This requires that the organization have a plan and program for service continuity, assign adequate and sufficient resources to the plan and program, and have the requisite infrastructure to carry out the plan and program. Based on risk appetite and tolerance, the organization must determine which service continuity plans it needs to establish, develop the plans, and exercise them on a regular and sufficient basis to ensure they remain viable as long as the service is vital to the organization.

The organization also must consider the range of service continuity activities. Business continuity or contingency plans are developed and implemented to sustain a high-value service, while recovery and restoration plans are focused on bringing services back to an acceptable level of business as usual. To ensure that all plans can be executed at will when called upon, the organization must also develop sufficient logistics and delivery capabilities.

Before the organization can develop, exercise, and position service continuity plans for implementation, several other organizational activities must occur. These include

- identification of the high-value services and associated assets for which service continuity plans must be developed *(This is addressed in the Enterprise Focus and Asset Definition and Management process areas.)*
- the potential hazards or risks to these high-value services and assets *(This is addressed in the Vulnerability Analysis and Resolution and Risk Management process areas.*)
- the consequences of these risks to the organization and its susceptibility to them *(This is addressed in the Risk Management process area.)*

In managing operational risk and resilience, the Service Continuity process area is complementary to Controls Management. Controls Management focuses on "condition management" to prevent risk, while Service Continuity directs the organization's attention to

"consequence management" or planning for managing the consequences of risks that are realized. Together, these process areas provide a comprehensive, coordinated, optimized, and holistic approach to managing asset and service resilience.

Related Process Areas

The development, implementation, and management of an internal control system to prevent risks and disruptive events is addressed in the Controls Management process area.

The identification and management of incidents that may require the execution of a service continuity plan is addressed in the Incident Management and Control process area.

Providing training for staff involved in service continuity plan testing and execution is addressed in the Organizational Training and Awareness process area.

The identification and prioritization of the organization's high-value services as a strategic planning activity is addressed in the Enterprise Focus process area.

The consideration of consequences as a foundational element for developing a service continuity plan is addressed in the Risk Management process area.

The association of assets to the high-value services they support is performed in the Asset Definition and Management process area.

The development, implementation, and management of strategies for technology asset availability and integrity is addressed in the Technology Management process area.

The identification of vital records and databases for service continuity is addressed in the Knowledge and Information Management process area.

The resilience considerations of the organization's reliance on public services and public infrastructure are addressed in the Environmental Control process area.

Summary of Specific Goals and Practices

Goals	Practices
SC:SG1 Prepare for Service Continuity	SC:SG1.SP1 Plan for Service Continuity
	SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity
SC:SG2 Identify and Prioritize High-Value Services	SC:SG2.SP1 Identify the Organization's High-Value Services
	SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies
	SC:SG2.SP3 Identify Vital Organizational Records and Databases
SC:SG3 Develop Service Continuity Plans	SC:SG3.SP1 Identify Plans to be Developed
	SC:SG3.SP2 Develop and Document Service Continuity Plans
	SC:SG3.SP3 Assign Staff to Service Continuity Plans
	SC:SG3.SP4 Store and Secure Service Continuity Plans
	SC:SG3.SP5 Develop Service Continuity Plan Training
SC:SG4 Validate Service Continuity Plans	SC:SG4.SP1 Validate Plans to Requirements and Standards
	SC:SG4.SP2 Identify and Resolve Plan Conflicts
SC:SG5 Exercise Service Continuity Plans	SC:SG5.SP1 Develop Testing Program and Standards
	SC:SG5.SP2 Develop and Document Test Plans
	SC:SG5.SP3 Exercise Plans
	SC:SG5.SP4 Evaluate Plan Test Results
SC:SG6 Execute Service Continuity Plans	SC:SG6.SP1 Execute Plans
	SC:SG6.SP2 Measure the Effectiveness of the Plan in Operation
SC:SG7 Maintain Service Continuity Plans	SC:SG7.SP1 Establish Change Criteria
	SC:SG7.SP2 Maintain Changes to Plans

Specific Practices by Goal

SC:SG1 Prepare for Service Continuity

The organizational processes for sustainability planning and execution are established.

SC:SG1.SP1 Plan for Service Continuity

Planning is performed for developing and implementing the organization's service continuity process.

SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity

The guidelines and standards for service continuity are established and communicated.

SC:SG2 Identify and Prioritize High-Value Services

The services that are required to meet the organization's mission are identified and prioritized.

SC:SG2.SP1 Identify the Organization's High-Value Services

The high-value services of the organization and their associated assets are identified.

SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies

The internal and external relationships necessary to ensure service continuity are identified and analyzed.

SC:SG2.SP3 Identify Vital Organizational Records and Databases

Vital information required for service continuity is identified.

SC:SG3 Develop Service Continuity Plans

Service continuity plans for high-value organizational services are developed.

SC:SG3.SP1 Identify Plans to be Developed

Required service continuity plans are identified.

SC:SG3.SP2 Develop and Document Service Continuity Plans

The required service continuity plans are developed and documented.

SC:SG3.SP3 Assign Staff to Service Continuity Plans

Staff members are assigned to the service continuity plans to ensure effective execution.

SC:SG3.SP4 Store and Secure Service Continuity Plans

Service continuity plans are stored and made accessible to those who have a need to know.

SC:SG3.SP5 Develop Service Continuity Plan Training

Training in the service continuity plans is developed and administered.

SC:SG4 Validate Service Continuity Plans

Service continuity plans are validated to ensure they satisfy requirements and standards and to resolve conflict between plans.

SC:SG4.SP1 Validate Plans to Requirements and Standards

Service continuity plans are examined to ensure they satisfy requirements and standards.

SC:SG4.SP2 Identify and Resolve Plan Conflicts

Conflicts between service continuity plans are identified and resolved.

SC:SG5 Exercise Service Continuity Plans

Service continuity plans are tested to ensure they meet their stated objectives.

SC:SG5.SP1 Develop Testing Program and Standards

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

SC:SG5.SP2 Develop and Document Test Plans

Service continuity test plans are developed and documented.

SC:SG5.SP3 Exercise Plans

Service continuity plans are exercised on a regular basis and results are documented.

SC:SG5.SP4 Evaluate Plan Test Results

Opportunities for improving service continuity plans are identified and implemented as a result of testing.

SC:SG6 Execute Service Continuity Plans

Service continuity plans are executed and reviewed.

SC:SG6.SP1 Execute Plans

Service continuity plans are executed as required.

SC:SG6.SP2 Measure the Effectiveness of the Plan in Operation

Post-execution review is performed to identify corrective actions.

SC:SG7 Maintain Service Continuity Plans

Changes to service continuity plans are identified and managed.

SC:SG7.SP1 Establish Change Criteria

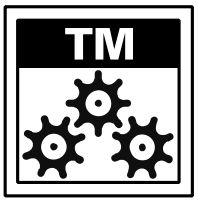
Change criteria for service continuity plans are established.

SC:SG7.SP2 Maintain Changes to Plans

Changes are made to service continuity plans as conditions dictate.

TECHNOLOGY MANAGEMENT

Operations



Purpose

The purpose of Technology Management is to establish and manage an appropriate level of controls related to the integrity and availability of technology assets to support the resilient operations of organizational services.

Introductory Notes

Technology is a pervasive organizational asset. Few organizational services are untouched by some aspect of technology—hardware, software, systems, tools, and infrastructure (such as networks) that support services. Technology assets directly support the automation (and efficiency) of services and are often inextricably tied to information assets because they provide the platforms on which information is stored, transported, or processed. For some organizations, technology is a prominent driver in accomplishing the mission and is considered a strategic element. Technology tends to be pervasive across all functions of the organization and therefore can be a significant contributor to strategic and competitive success.

From a broad perspective, technology describes any technology component or asset that supports or automates a service and facilitates its ability to accomplish its mission. Examples of technology assets include software, hardware, and firmware, including physical interconnections between these assets such as cabling. Technology has many layers, some which are specific to a service (such as an application system) and others which are shared by the organization (such as the enterprise-wide network infrastructure) to support more than one service. Organizations must describe technology assets sufficiently to facilitate development and satisfaction of resilience requirements. In some organizations, this may be at the application system level; in others, it might be more granular, such as at the server or personal computer level.

The Technology Management process area addresses the importance of technology assets in the operational resilience of services, as well as unique issues specific to technology such as integrity and availability management. In this process area, technology assets are prioritized according to their value in supporting high-value organizational services. Physical, technical, and administrative controls that keep technology assets viable and sustainable are selected, implemented, and managed, and the effectiveness of these controls is monitored. In addition, technology asset risks are identified and mitigated in an attempt to prevent disruption where possible.

The integrity of technology assets is addressed through mastery of capabilities such as configuration, change, and release management. The availability of technology assets, critical for supporting the resilience of services, is established and managed by controlling the operational environment in which the assets operate, by performing regular maintenance on these assets, and by limiting the potential effects of interoperability issues. Because technology assets may extend outside of the physical and logical boundaries of the

organization, the organization must address the interaction with external entities that provide technology assets or support for technology assets to the organization.

Related Process Areas

The establishment and management of resilience requirements for technology assets are performed in the Resilience Requirements Development and Resilience Requirements Management process areas.

The identification, definition, management, and control of technology assets are addressed in the Asset Definition and Management process area.

The risk management cycle for technology assets is addressed in the Risk Management process area.

The management of the internal control system that ensures the protection of technology assets is addressed in the Controls Management process area.

The selection, implementation, and management of access controls for technology assets is performed in the Access Management process area.

The development of service continuity plans for technology assets is performed in the Service Continuity process area.

The establishment and management of relationships with external entities to ensure the resilience of services that are executed in facilities they own and operate are addressed in the External Dependencies Management process area.

Summary of Specific Goals and Practices

Goals	Practices
TM:SG1 Establish and Prioritize Technology Assets	TM:SG1.SP1 Prioritize Technology Assets
	TM:SG1.SP2 Establish Resilience-Focused Technology Assets
TM:SG2 Protect Technology Assets	TM:SG2.SP1 Assign Resilience Requirements to Technology Assets
	TM:SG2.SP2 Establish and Implement Controls
TM:SG3 Manage Technology Asset Risk	TM:SG3.SP1 Identify and Assess Technology Asset Risk
	TM:SG3.SP2 Mitigate Technology Risk
TM:SG4 Manage Technology Asset Integrity	TM:SG4.SP1 Control Access to Technology Assets
	TM:SG4.SP2 Perform Configuration Management
	TM:SG4.SP3 Perform Change Control and Management
	TM:SG4.SP4 Perform Release Management
TM:SG5 Manage Technology Asset Availability	TM:SG5.SP1 Perform Planning to Sustain Technology Assets
	TM:SG5.SP2 Manage Technology Asset Maintenance
	TM:SG5.SP3 Manage Technology Capacity
	TM:SG5.SP4 Manage Technology Interoperability

TM:SG1 Establish and Prioritize Technology Assets

Technology assets are prioritized to ensure the resilience of the high-value services that they support.

TM:SG1.SP1 Prioritize Technology Assets

Technology assets are prioritized relative to their importance in supporting the delivery of high-value services.

TM:SG1.SP2 Establish Resilience-Focused Technology Assets

Technology assets that specifically support execution of service continuity and service restoration plans are identified and established.

TM:SG2 Protect Technology Assets

Administrative, technical, and physical controls for technology assets are identified, implemented, monitored, and managed.

TM:SG2.SP1 Assign Resilience Requirements to Technology Assets

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

TM:SG2.SP2 Establish and Implement Controls

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

TM:SG3 Manage Technology Asset Risk

Operational risks to technology assets are identified and managed.

TM:SG3.SP1 Identify and Assess Technology Asset Risk

Risks to technology assets are identified and assessed.

TM:SG3.SP2 Mitigate Technology Risk

Risk mitigation strategies for technology assets are developed and implemented.

TM:SG4 Manage Technology Asset Integrity

The integrity of technology assets is managed.

TM:SG4.SP1 Control Access to Technology Assets

Access to technology assets is controlled.

TM:SG4.SP2 Perform Configuration Management

The configuration of technology assets is managed.

TM:SG4.SP3 Perform Change Control and Management

Changes to technology assets are managed.

TM:SG4.SP4 Perform Release Management

The iteration of technology assets placed into the production environment is managed.

TM:SG5 Manage Technology Asset Availability

The availability of technology assets to support high-value services is managed.

TM:SG5.SP1 Perform Planning to Sustain Technology Assets

The availability and functionality of high-value technology assets is ensured through developing plans to sustain them.

TM:SG5.SP2 Manage Technology Asset Maintenance

Operational maintenance is performed on technology assets.

TM:SG5.SP3 Manage Technology Capacity

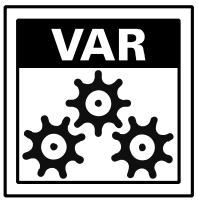
The operating capacity of technology assets is managed.

TM:SG5.SP4 Manage Technology Interoperability

The interoperability of technology assets is managed.

VULNERABILITY ANALYSIS AND RESOLUTION

Operations



Purpose

The purpose of Vulnerability Analysis and Resolution is to identify, analyze, and manage vulnerabilities in an organization's operating environment.

Introductory Notes

A vulnerability is the susceptibility of an asset and associated service to disruption. Examples of vulnerabilities are weaknesses in the physical or technical infrastructure of the organization and flaws in the character of an individual employee. All assets of the organization that are operationally deployed—people, information, technology, and facilities—are subject to some level and type of vulnerability.

Vulnerabilities can result in operational risks and must be identified and remediated to avoid disruptions to the organization's ability to meet its strategic objectives. Vulnerability analysis and resolution is a complementary activity to risk management. It requires that an organization identify weaknesses to its assets and services and understand the potential impact to the organization when these weaknesses are exploited.

As organizations have grown more dependent on their technical infrastructures, there has been a corresponding increase in focus on identifying only technical vulnerabilities. However, operational risk emanates from weaknesses in the protection of *all* types of assets, and thus the vulnerability analysis and resolution activity must cover not only weaknesses in the technical infrastructure but also potential threats to the viability of people, information, and facilities.

The identification and remediation of technical vulnerabilities is a means for mitigating operational risk, but it does not fully constitute the activities of risk management. Instead, vulnerability analysis and resolution informs the organization of threats that must be analyzed in the risk management process to determine whether they pose tangible risk to the organization based on its unique risk drivers, appetite, and tolerance. In turn, the risk management process informs vulnerability analysis and resolution processes to focus attention on the assets and services that are most critical to meeting strategic objectives.

The Vulnerability Analysis and Resolution process area describes the organization's ability to establish a vulnerability management strategy and to efficiently and effectively assign enterprise-wide resources to implement that strategy. The organization identifies and analyzes vulnerabilities across the enterprise and communicates relevant information about these vulnerabilities to other organizational processes that require this information. Strategies are developed to reduce the organization's exposure to vulnerabilities. In this way, the organization is mitigating risk where the exploited vulnerability has the potential to impact the organization.

Vulnerability Analysis and Resolution provides the organization an important opportunity to improve processes that may introduce vulnerabilities into the operating environment. Vulnerabilities are logged and tracked, and root-cause analysis and trending is performed on

them to determine if breakdowns in other organizational processes are resulting in exposure. This knowledge is translated into improved strategies for protecting and sustaining assets and services as well as improvements in the processes.

Vulnerabilities may result in events and incidents that the organization must manage. The Incident Management and Control process area addresses the processes for identifying, analyzing, handling, and responding to incidents.

Vulnerability identification and analysis is an important source of potential risks to the organization. Risks are identified, analyzed, and mitigated (through vulnerability reduction activities) in the Risk Management process area.

Related Process Areas

The risk management cycle for organizational services, processes, and assets is addressed in the Risk Management process area.

Monitoring for events, incidents, and vulnerabilities is addressed in the Monitoring process area.

Summary of Specific Goals and Practices

Goals	Practices
VAR:SG1 Prepare for Vulnerability Analysis and Resolution	VAR:SG1.SP1 Establish Scope
	VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy
VAR:SG2 Identify and Analyze Vulnerabilities	VAR:SG2.SP1 Identify Sources of Vulnerability Information
	VAR:SG2.SP2 Discover Vulnerabilities
	VAR:SG2.SP3 Analyze Vulnerabilities
VAR:SG3 Manage Exposure to Vulnerabilities	VAR:SG3.SP1 Manage Exposure to Vulnerabilities
VAR:SG4 Identify Root Causes	VAR:SG4.SP1 Perform Root-Cause Analysis

Specific Practices by Goal

VAR:SG1 Prepare for Vulnerability Analysis and Resolution

Preparation for vulnerability analysis and resolution activities is conducted.

VAR:SG1.SP1 Establish Scope

The assets and operational environments that must be examined for vulnerabilities are identified.

VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy

Establish and maintain an operational vulnerability analysis and resolution strategy.

VAR:SG2 Identify and Analyze Vulnerabilities

Establish and maintain a process for identifying and analyzing vulnerabilities.

VAR:SG2.SP1 Identify Sources of Vulnerability Information

The sources of vulnerability information are identified.

VAR:SG2.SP2 Discover Vulnerabilities

A process is established to actively discover vulnerabilities.

VAR:SG2.SP3 Analyze Vulnerabilities

Vulnerabilities are analyzed to determine whether they need to be reduced or eliminated.

VAR:SG3 Manage Exposure to Vulnerabilities

Strategies are developed to manage exposure to identified vulnerabilities.

VAR:SG3.SP1 Manage Exposure to Vulnerabilities

Strategies are developed and implemented to manage exposure to identified vulnerabilities.

VAR:SG4 Identify Root Causes

The root causes of vulnerabilities are examined to improve vulnerability analysis and resolution and reduce organizational exposure.

VAR:SG4.SP1 Perform Root-Cause Analysis

Perform review of identified vulnerabilities to determine and address underlying causes.

Appendix A: Generic Goals and Practices

This document describes the generic goals and practices that the organization deploys to attain successively improving degrees of process institutionalization and capability for operational resilience management. These practices exhibit the organization's commitment and ability to perform operational resilience management processes, as well as its ability to measure performance and verify implementation.

Except where otherwise noted, generic goals and practices are applied universally across all process areas throughout the CERT Resilience Management Model. In some cases, generic goals and practices mirror process areas in the model. This occurs because some of the practices contained in process areas are also useful in improving and sustaining process maturity. Where this occurs, there are references to the process area that is reflected in the generic practices.

GG1 Achieve Specific Goals

The operational resilience management process supports and enables achievement of the specific goals of the process area by transforming identifiable input work products to produce identifiable output work products.

GG1.GP1 Perform Specific Practices

Perform the specific practices of the process area to develop work products and provide services to achieve the specific goals of the process area.

This practice requires the organization to perform the practices, produce the work products, and deliver the services that are contained in the process definition for a process area. The organization may perform these practices in an improvised or reactive manner, and there may not be any process definition to support the performance of the practices. The degree to which the performance of practices is formalized varies from organization to organization and may be inconsistent within an organization. The success of achieving the work products and delivering the service of the practices may be directly related to the staff involved in the process.

GG2 Institutionalize a Managed Process

The process is institutionalized as a managed process.

GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the process.

This practice establishes the foundation for higher level managers' responsibility for overseeing, directing, and guiding the operational resilience management process. Higher level managers set expectations for managing operational resilience in this practice and communicate these expectations to those who are responsible as appropriate. Regular reviews of operational resilience activities are performed and reported to higher level managers for interpretation. Higher level managers make recommendations where gaps are perceived in process performance.

The behavioral expectations of higher level managers are instantiated in organizational policies that address operational resilience management, as well as in expectations for planning and performing operational resilience processes.

Higher level managers are also responsible for ensuring appropriate levels of compliance with legal, regulatory, contractual, and government obligations.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management process.

Subpractices

1. Establish governance over operational resilience activities.

   The organization's governance activity is expanded to include oversight over the activities and processes that the organization uses to manage operational resilience and to perform the process.

2. Develop and publish organizational policy for operational resilience management.

   Establish the organizational expectations for planning and performing the process, and communicate these expectations via policy. The policy should reflect higher level managers' objectives for the process.

GG2.GP2 Plan the Process

Establish and maintain the plan for performing the process.

In this practice, the organization determines what is needed to perform the operational resilience management process and to achieve the established objectives, to prepare a plan for performing the process, to prepare a process description, and to get agreement on the plan from relevant stakeholders. In some cases, this generic practice may be applied to a planning process in a particular process area; in that case, this generic practice sets an expectation that the planning process itself needs to be planned.

Establishing a plan includes documenting the plan and providing a process description, *as well as assigning ownership* of the plan with requisite authority to carry out the plan. Maintaining the plan includes changing it as necessary to reflect corrective actions, changes in requirements, or improvements.

The plan for the process should be directly influenced by the strategic and operational planning processes of the organization and reflect strategic objectives and initiatives where appropriate.

The plan for performing the process typically includes the following elements and activities:

- process description
- standards and requirements for the work products and services of the process
- specific objectives for the performance of the process
- dependencies among the activities, work products, and services of the process
- the assignment of resources (typically funding, people, and tools) needed to perform the process
- assignment of responsibility and authority
- training needed to perform and support the process
- work products to be controlled and the level of control to apply
- measurement requirements to provide insight into the performance of the process, its work products, and its services
- involvement of identified stakeholders
- activities for monitoring and controlling the process
- activities for objectively evaluating the process
- activities for management review of the process and the work products

Refer to the Enterprise Focus process area for more information about creating, resourcing, and implementing a strategic resilience plan and establishing a resilience program.

Refer to individual process areas for specific guidance on creating, implementing, and managing plans, where relevant.

Subpractices

1. Define and document the plan for performing the process.

   This plan may be a stand-alone document, embedded in a more comprehensive document, or distributed across multiple documents. In the case of the plan being distributed across multiple documents, ensure that a coherent picture of who does what is preserved.

2. Define and document the process description.

   The process description, which includes relevant standards and procedures, may be included as part of the plan for performing the process or may be included in the plan by reference.

3. Review the plan with relevant stakeholders and get their agreement.

   Review the planned process to ensure that it satisfies policy (and the requirements for governance), plans, requirements, and standards to provide assurance to stakeholders.

4. Revise the plan as necessary.

GG2.GP3 Provide Resources

Provide adequate resources for performing the process, developing the work products, and providing the services of the process.

This practice focuses on providing the resources necessary to perform the process as defined by the plan and ensuring that resources are available when needed. Resources are formally identified and assigned to process plan elements.

Resources include an adequate number of skilled staff, expense and capital funding, facilities, and tools, techniques, and methods. The interpretation of the term "adequate" depends upon many factors and can change over time. Inadequate resources may be addressed by increasing resources or by removing requirements, constraints, and commitments.

Subpractices

1. Staff the process.

   Ensure that a sufficient and adequate level of human resources is available and appropriately skilled to perform the process.

   Staff responsible for performing process activities may be different from those responsible for evaluating the performance of the process.

   Refer to the Organizational Training and Awareness process area for information about training staff for resilience-focused roles and responsibilities.

   Refer to the Human Resource Management process area for information about the acquisition of staff to fulfill roles and responsibilities.

2. Fund the process.

   Funding must be earmarked and provided to support the goals and objectives of operational resilience management processes. Funding is an indication of higher level managers' support and sponsorship of the process.

   At a minimum, funding must be available to support proper oversight of the process. This includes (a) establishing and maintaining an appropriate internal control system for services and related assets and (b) periodic reporting of key indicators and metrics to assess process performance.

   Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for operational resilience management processes.

3. Provide the necessary tools, techniques, and methods to perform the process.

GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the process, developing the work products, and providing the services of the process.

This practice ensures that there is accountability and responsibility for performing the process and ensuring the achievement of expected results throughout the life of the process. The people assigned must have the appropriate authority to act and to perform the assigned responsibilities.

Responsibility can be assigned and tracked through job descriptions, the process plan, or other means, such as performance management (goals and performance reviews).

Refer to the Human Resource Management process area for more information about establishing resilience as a job responsibility, developing resilience-related performance goals and objectives, and measuring and assessing performance against these goals and objectives.

Subpractices

1. Assign responsibility and authority for performing the process.

   Organizations may establish an operational resilience management process group to take responsibility for the overall operational resilience management process, including any specific process. This group may also formally interface with higher level managers for the purpose of reporting on organizational progress against process goals as part of the governance process for operational resilience management.

2. Assign responsibility and authority for performing the specific tasks of the process.

3. Confirm that people assigned with responsibility and authority understand it and are willing and able to accept it.

GG2.GP5 Train People

Train the people performing or supporting the process as needed.

This practice ensures that the necessary staff have the skills and expertise to perform or support the process. The skills necessary to perform the process are documented in the plan and compared to the available resources. Training needs are identified to address skill gaps.

Appropriate training is provided to the staff who perform the work. Overview training is provided to those who interact with those performing the work.

Refer to the Organizational Training and Awareness process area for more information about training the people performing or supporting the process.

Refer to the Human Resource Management process area for more information about inventorying skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.
2. Identify process skill gaps based on available resources and their current skill levels.
3. Identify training opportunities to address skill gaps.
4. Provide training and review the training needs as necessary.

GG2.GP6 Manage Work Product Configurations

Place designated work products of the process under appropriate levels of control.

The purpose of this practice is to establish and maintain the integrity of the designated work products of the process (or their descriptions) throughout their useful life. Work products of the process must be managed and controlled as operating conditions change and evolve.

The designated work products are specifically identified in the plan for performing the process, along with a specification of the appropriate level of control.

Different levels of control are appropriate for different work products and for different points in time. For some work products, it may be sufficient to maintain version control (i.e., the version of the process work product in use at a given time, past or present, is known, and changes are incorporated in a controlled manner). Version control is usually under the sole control of the owner of the process work product (typically an individual, group, or team).

Sometimes it may be critical for work products to be placed under formal or baseline configuration management. This type of control includes defining and establishing baselines at predetermined points. These baselines are formally reviewed and agreed upon and serve as the basis for further development and use of the process work product.

Additional levels of control between version control and formal configuration management are possible. An identified work product may be under various levels of control at different points in time.

Because change control, version control, and configuration management are fundamental activities in many operational resilience management processes, this generic practice also addresses the processes and practices necessary to establish baseline work products (e.g., developing an asset database) and for performing change control on these work products as the operational environment changes and evolves. In some cases, the management of work products is critical to the operational resilience management process and therefore is included in the specific practices of the process area, ranging from simple change control activities to baseline-driven configuration management. Examples of these practices can be found throughout process areas such as Access Management, Asset Definition and Management, and Incident Management and Control.

Configuration management of technical assets (such as software, hardware, and systems) as traditionally understood in the context of managing information technology is addressed as a specific operational resilience management practice in the Technology Management process area.

GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the process as planned.

In this practice, the expected involvement of stakeholders is established, planned, and maintained during the execution of a process.

Stakeholders are involved in various activities in a process. Their roles should be considered in the process plan, and could include

- planning
- decision making
- commitments
- communications
- coordination
- review
- appraisal
- requirements definition and documentation
- resolution of problems

The objective of planning stakeholder involvement is to ensure that interactions necessary to the process are accomplished without excessive numbers of affiliated groups and individuals impeding process execution.

In some process areas, the identification and inclusion of stakeholders in the process is critical to process success. In these areas, specific practices or subpractices have been included to address stakeholder involvement, particularly where processes reach extensively into the organization, such as in the Monitoring and Communications process areas.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Relevant stakeholders are identified among the suppliers of inputs to, the users of outputs from, and the performers of activities within the process. Once the relevant stakeholders are identified, the appropriate level of their involvement in process activities is planned.

2. Communicate the list of these stakeholders to planners and those responsible for process performance.

3. Involve relevant stakeholders in the process as planned.

GG2.GP8 Monitor and Control the Process

Monitor and control the process against the plan for performing the process and take appropriate corrective action.

The purpose of this practice is to perform the direct day-to-day monitoring and controlling of the process. Appropriate visibility into the process is maintained so that appropriate corrective action can be taken when necessary. Monitoring and controlling the process involves establishing appropriate metrics and measuring appropriate attributes of the process or work products produced by the process. The metrics and measurements may be qualitative or quantitative as appropriate.

Refer to the Monitoring process area for more information about collecting, organizing, and distributing data that may be useful for monitoring and controlling processes.

Refer to the Measurement and Analysis process area for more information about establishing process metrics and measurement.

Refer to the Enterprise Focus process area for more information about providing process information to managers, identifying issues, and determining appropriate corrective actions.

Subpractices

1. Measure actual performance against the plan for performing the process.

   The measures are of the process, its work products, and its services.

2. Review accomplishments and results of the process against the plan for performing the process.

3. Review activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues.

   The reviews are intended to provide the immediate level of managers with appropriate visibility into the process. The reviews can be both periodic (for example, planned as part of a regular audit of the organization's internal control system) and event driven.

   Process reviews are likely to concentrate on the effectiveness and efficiency of the internal control system for services and assets, as well as the satisfaction of service and asset resilience requirements.

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.

5. Identify problems in the plan for performing and executing the process.

6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.

   New risks that could be introduced or affect the mitigation plans for existing risks should be considered before any corrective action is taken. *Refer to the Risk Management process area for more information about managing risk.*

   Corrective actions may include the following:

- taking remedial action to repair defective work products or services
- changing the plan for performing the process
- adjusting resources (people, tools, etc.)
- negotiating changes to the established commitments
- securing change to the requirements and objectives that have to be satisfied
- terminating the effort

If corrective action is required, further analysis may be necessary to identify improvements to the process.

7. Track corrective action to closure.

GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the process against its process description, standards, and procedures and address noncompliance.

The purpose of this practice is to provide assurance that the process is implemented as planned and adheres to its process description, standards, and procedures as evidenced through an evaluation of selected work products of the process. The evaluation must be independent; that is, those directly involved in the performance of the process cannot perform the objective evaluation or render an opinion on adherence.

Activities such as internal and external audits, post-event reviews, and capability appraisals allow the organization to have an independent and objective evaluation of the effectiveness of the risk management process, adherence to the process, and identification of areas of noncompliance.

Objectively evaluating adherence is especially important under times of stress (such as during incident response) to ensure that the organization is relying on processes and not reverting to ad hoc practices that require people and technology as their basis.

GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the process with higher level managers and resolve issues.

As a part of governing the operational resilience management process, higher level managers are provided with the appropriate visibility into the process.

Higher level managers includes those in the organization above the immediate level of managers responsible for the process. This information is provided to help higher level managers to provide and enforce policy for the process, as well as to perform overall guidance. (This practice is not performed to help those who perform the direct day-to-day monitoring and controlling of the process.)

Different managers have different needs for information about the process. These reviews help ensure that informed decisions on the planning and

performing of the process can be made. Therefore, these reviews are expected to be both periodic and event driven.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management process.

GG3 Institutionalize a Defined Process

The process is institutionalized as a defined process.

GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined process.

The purpose of this generic practice is to establish and maintain a description of the process that is tailored from the organization's set of standard processes to address the needs of a specific organizational unit or line of business. The organization should have standard processes that define the specific operational resilience management capability, along with guidelines for tailoring these processes to meet the needs of a specific organizational unit or line of business, or any other organizationally defined operating division.

Managing the operational resilience management process is an enterprise concern that is typically carried out at the enterprise level, given that it must reflect the strategic and performance objectives for the organization. That said, aspects of the process must be tailorable and adaptable at the organizational unit or line of business level to ensure that appropriate process activities occur throughout the organization.

To achieve consistency of process application, the tailored definition of processes used at local levels must be consistent with and reflect the enterprise philosophy and strategy. This consistency allows the organization to track performance, mitigate risks within defined risk parameters, and derive benefits (e.g., efficiencies, value, and cost savings) at the enterprise level. It also ensures minimal variability as the process is performed across the enterprise, allowing for the sharing of process assets, work products, data, and learning. Otherwise, the execution of process activities at local levels will be inconsistent and variable, resulting in inefficiencies and ineffectiveness of these activities at the enterprise level.

Subpractices

1. Select from the organization's set of standard processes those processes that cover the process area and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization's tailoring guidelines.
3. Ensure that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.

5. Revise the description of the defined process as necessary.

GG3.GP2 Collect Improvement Information

Collect work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.

The purpose of this generic practice is to collect information and work products derived from planning and performing the process. This generic practice is performed so that the information and work products can be included in the organizational process assets and made available to those who are planning and performing the same or similar processes. The information and work products are stored in the organization's measurement repository and its process asset library.

Subpractices

1. Store process and work product measures in the organization's measurement repository.

   The process and work product measures are primarily those that are defined in the common set of measures for the organization's set of standard processes.

2. Submit documentation for inclusion in the organization's process asset library.
3. Document lessons learned from the process for inclusion in the organization's process asset library.
4. Propose improvements to the organizational process assets.

Appendix B: Targeted Improvement Roadmaps

Achieving FISMA Compliance

A suggested targeted improvement roadmap[13] for using CERT-RMM to achieve FISMA compliance is provided below.

Required CERT-RMM Process Areas			Association with FISMA, NIST Supporting Documents	Notes
Category	**Process Area**	**Minimum Required Capability Level**		
Operations	Access Management (AM)	Level 2[14]	FISMA – Select Security Controls FISMA – Implement Security Controls FIPS 200 NIST SP 800-53 NIST SP 800-70 OMB Memorandum M-10-15	Strong connection to Identity Management in CERT-RMM
Engineering	Asset Definition and Management (ADM)	Level 2	FISMA – Categorize Information Systems FIPS 199 NIST SP 800-60 OMB Memorandum M-10-15	Level 1 base practices in ADM more broadly cover all asset types—people, information, technology, and facilities—while FISMA is focused on information systems.
Enterprise Management	Enterprise Focus (EF)	Level 1	FISMA – Establish Organizational View NIST SP 800-39 OMB Memorandum M-10-15	Level 1 base practices in CERT-RMM are more extensive than required by FISMA or NIST 800-39's ~~o~~rganizational view."

[13] See page 69 for more information about using CERT-RMM targeted improvement roadmaps.

[14] Because of the FISMA emphasis on policies and procedures to support security programs, these process areas are raised to level 2 capability in CERT-RMM, which addresses elements of process capability (such as policy, governance, resources, training, monitoring, and control) that support a ~~m~~managed" level of operational resilience management. Without FISMA policy requirements, these capability levels could be established at level 1.

Required CERT-RMM Process Areas			Association with FISMA, NIST Supporting Documents	Notes
Category	**Process Area**	**Minimum Required Capability Level**		
Operations	Environmental Control (EC)	Level 2	FISMA – Select Security Controls FISMA – Implement Security Controls FIPS 200 NIST SP 800-53 NIST SP 800-70	EC addresses security controls specifically for *facility* assets. EC also addresses dependencies on public services and public infrastructure (e.g., telecommunications, utilities, emergency management, and first responder services).
Operations	Identity Management (ID)	Level 2	FISMA – Select Security Controls FISMA – Implement Security Controls FIPS 200 NIST SP 800-53 NIST SP 800-70 OMB Memorandum M-10-15	Strong connection to Access Management in CERT-RMM
Operations	Incident Management and Control (IMC)	Level 2	FISMA General Requirements NIST SP 800-61 OMB Memorandum M-07-16 OMB Memorandum M-06-19 OMB Memorandum in support of Executive Order 13402 OMB Memorandum M-10-15	Supports FISMA incident management and handling provision
Operations	Knowledge and Information Management (KIM)	Level 2	FISMA – Select Security Controls FISMA – Implement Security Controls FIPS 200 NIST SP 800-53 NIST SP 800-70	KIM addresses security controls specifically for *information* assets.
Engineering	Controls Management (CTRL)	Level 2	FISMA –Assess Security Controls NIST SP 800-37 NIST SP 800-39 NIST 800-53A OMB Memorandum M-10-15	Level 2 capability for controls management exceeds FISMA requirements and extends to all asset types, not just information systems.

Required CERT-RMM Process Areas			Association with FISMA, NIST Supporting Documents	Notes
Category	**Process Area**	**Minimum Required Capability Level**		
Process Management	Monitoring (MON)	Level 2	FISMA – Assess Security Controls FISMA – Monitor Security State NIST SP 800-37 NIST SP 800-53A OMB Memorandum M-10-15	Supports the process of continuous real-time monitoring
Enterprise Management	Organizational Training and Awareness (OTA)	Level 1	FISMA General Requirements	Supports FISMA security awareness and training provision; CERT-RMM level 1 base practices are more extensive than required by FISMA.
Enterprise Management	Risk Management (RISK)	Level 2	FISMA – Categorize Information Systems FISMA – Implement Security Controls FIPS 199 NIST 800-30 NIST SP 800-60 OMB Memorandum M-10-15	Level 2 capability for risk management exceeds FISMA requirements and extends to all asset types, not just information systems.
Engineering	Resilience Requirements Definition (RRD)	Level 1	FISMA – Categorize Information Systems FIPS 199 NIST SP 800-60	Level 1 base practices in CERT-RMM are more extensive than required by FISMA.
Operations	Service Continuity (SC)	Level 2	FISMA – Select Security Controls FISMA – Implement Security Controls FISMA – Assess Security Controls FIPS 200 NIST SP 800-53 NIST SP 800-53A NIST SP 800-70	Supports FISMA continuity of operations provision

Required CERT-RMM Process Areas			Association with FISMA, NIST Supporting Documents	Notes
Category	**Process Area**	**Minimum Required Capability Level**		
Operations	Technology Management (TM)	Level 2	FISMA – Select Security Controls FISMA – Develop System Configuration Requirements FISMA – Implement Security Controls FIPS 200 NIST SP 800-53 NIST SP 800-70	TM addresses security controls specifically for *technology* assets including software, hardware, systems, and networks
Operations	Vulnerability Analysis and Resolution (VAR)	Level 2	FISMA – Assess Security Controls FISMA – Monitor Security State NIST SP 800-53A NIST SP 800-37 OMB Memorandum M-10-15	Considered part of FISMA risk management, although is a separate process in CERT-RMM

Managing Cloud Computing

A suggested (but not all-inclusive) targeted improvement roadmap for determining how well the organization is managing the potential risks when using cloud computing services is provided below.

Process Areas	Selection Rationale
Asset Definition and Management	Asset Definition and Management (ADM) is focused on the resilience of service-critical assets. Managing the risks from cloud computing means that the organization has processes in place to identify and document assets, establish ownership and custodianship for assets, and link assets to the services they support. The concept of asset ownership and custodianship are especially important in the cloud computing environment to establish clear lines of demarcation and responsibility for operational resilience.
External Dependencies Management	In External Dependencies Management (EXD), the organization's process for identifying, analyzing, and addressing the risks associated with the actions of service providers, the formalization of the relationship with such providers, and the ongoing management of provider relationships are established. An external dependency exists when an external entity has access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization. For cloud computing, managing external dependencies is an ongoing concern over the life of the relationship.

Process Areas	Selection Rationale
Risk Management	Risk Management (RISK) addresses the organization's cycle for identifying, analyzing, and mitigating operational risk. For cloud computing, this process area is focused specifically on how well the organization identifies, analyzes, and mitigates risk related to all sources and categories of operational risk, such as data privacy, regulatory compliance, and insider threats. This process area seeks to ensure that the organization also has the capability to manage the risk of unmet requirements from providers of cloud computing infrastructure, platforms, or software services.
Resilience Requirements Development	Resilience Requirements Development (RRD) broadly addresses the way in which the organization identifies, develops, implements, and manages resilience requirements to ensure that high-value assets are not disrupted. For cloud computing, resilience requirements form the basis for the selection of appropriate controls for protecting and sustaining assets. RRD ensures the organizational processes for developing the appropriate requirements, informs the process for control selection, and supplies defined requirements for formal agreements with the cloud service provider.
Resilience Requirements Management	Resilience Requirements Management (RRM) addresses the process used by the organization to manage resilience requirements as they change and evolve over time. For cloud computing, the effective management of requirements ensures that an agreed-to set of requirements between asset owners and asset custodians (service providers) is defined and managed. This includes establishing criteria for the evaluation, acceptance of, and communication about asset requirements between the organization and the cloud computing provider.
Technology Management	Technology Management (TM) addresses the management of operational risk to technology assets. It covers the technology operational life cycle—release management, protecting and sustaining technology assets, interoperability, capacity planning, and maintenance—and seeks to ensure that potential vulnerabilities and threats related to operating and maintaining hardware, software, systems, tools, and infrastructure (such as failing to control access to technology assets or not performing configuration management) do not pose risk to the integrity and availability of technology assets.
Knowledge and Information Management	Knowledge and Information Management (KIM) is focused on understanding the importance of high-value information to the organization's services. For cloud computing, this process area determines the organization's maturity in managing the confidentiality, integrity, and availability of intangible information. This includes implementing strategies to protect and sustain information assets (considering all the ways in which they are stored, transported, transmitted, and processed), such as proper duplication and retention to ensure availability of the information when needed.
Environmental Control	Environmental Control (EC) addresses the process used to manage an appropriate level of physical, environmental, and geographical controls to support the resilient operations of services in organizational facilities. Considerations for cloud computing include understanding the organization's dependence on public services, public infrastructure, and geographic location of data centers where services are performed.
Service Continuity	Service Continuity (SC) addresses the process used to develop, deploy, exercise, implement, and manage plans for responding to and recovering from disruptive events and restoring operations to business as usual. Considerations for cloud computing include ensuring the organization has sufficient capability to determine requirements for and oversee continuity of operations for cloud computing services.

Managing the Insider Threat Challenge

A suggested (but not all-inclusive) targeted improvement roadmap for determining how well the organization is managing the potential threat posed by trusted staff is provided below.

Process Area	Selection Rationale
Human Resource Management	Human Resource Management (HRM) addresses the management of operational risk posed by the processes for acquiring and severing staff. It covers the employment life cycle—hiring, performance management, and termination—and seeks to ensure that potential vulnerabilities and threats related to acquiring and managing staff (such as failing to identify a job candidate's criminal history or past credit problems) do not pose risk to the organization.
People Management	People Management (PM) is focused on minimizing the impact of the lack of availability of high-value staff on the organization's operational resilience. For insider threat, this process area determines the organization's maturity in identifying high-value staff (who could intentionally cause damage to the organization) and ensuring proper redundancy and succession planning if these staff are unavailable for any reason, including termination.
Risk Management	Risk Management (RISK) addresses the organization's cycle for identifying, analyzing, and mitigating risk. For insider threat, this process area is focused specifically on how well the organization identifies, analyzes, and mitigates risk related to the intentional, deliberate, or accidental actions of trusted staff, including employees and external entities (contractors, etc.).
Vulnerability Analysis and Resolution	In Vulnerability Analysis and Resolution (VAR), the organization's process for identifying, analyzing, and addressing potential threats to high-value assets is established. For insider threat, this process area is focused on the degree to which the organization can specifically identify areas of weakness that can be exploited by trusted staff. This process area also focuses on how well the organization identifies and manages vulnerabilities related to how staff are acquired, trained, deployed, and managed.
Controls Management	Controls Management (CTRL) broadly addresses the way in which the organization identifies, develops, implements, and manages controls (administrative, physical, and technical) to ensure that high-value assets are not disrupted. For insider threat, controls management is focused on managing the controls that specifically prevent trusted staff from intentionally, deliberately, or inadvertently disrupting high-value assets. In addition, this process area seeks to ensure that controls are implemented to manage potential vulnerabilities and threats posed by trusted staff who have special privileges (such as special levels of access to high-value assets).
Access Management	Access Management (AM) addresses the process used by the organization to enable access to high-value assets through the management of access privileges. For insider threat, the effective management of access privileges ensures that trusted staff members are provided only the level of access necessary to perform their assigned job responsibilities and that staff provided with special levels of access are provided those levels only when needed.

Glossary of Terms

This document contains an alphabetical glossary of terms for the CERT Resilience Management Model. The glossary provides definitions based on how the term is used in the context of operational resilience management. For this reason, the definitions provided may differ from those in common use.

The origin for each term is noted in brackets at the end of each definition. The notation refers to the operational resilience management process area where the term originates or is used. For example, [AM] refers to the Access Management process area.

Abuse case
See "misuse/abuse case."

Access acknowledgement
A form or process that allows users to acknowledge (in writing) that they understand their access privileges and will abide by the organization's policy regarding the assignment, use, and revocation of those privileges. [AM]

Access control
The administrative, technical, or physical mechanism that provides a "gate" at which identities must present proper credentials and be authenticated to pass. [AM] [KIM]

Access control policy or Access management policy
An organizational policy that establishes the policies and procedures for requesting, approving, and providing access to persons, objects, and entities and establishes the guidelines for disciplinary action for violations of the policy. [AM]

Access Management (AM)
An operations process area in CERT-RMM. The purpose of Access Management is to ensure that access granted to organizational assets is commensurate with their business and resilience requirements.

Access privilege
A mechanism for describing and defining an appropriate level of access to an organizational asset— information, technology, or facilities—commensurate with an identity's job responsibilities and the business and resilience requirements of the asset. [AM] [HRM]

Access request
A mechanism for requesting access to an organizational asset that is submitted to and approved by owners of the asset (with sufficient justification). [AM]

Acculturation
The acquisition and adoption of a process improvement mindset and culture for resilience throughout all levels of the organization. [HRM]

Adaptive maintenance
Maintenance performed to adapt a facility to a different operating environment. [EC]

Administrative control
A type of managerial control that ensures alignment to management's intentions and includes such artifacts as governance, policy, monitoring, auditing, separation of duties, and the development and implementation of service continuity plans. [KIM]

Agreement
A legal agreement between the organization and a business partner or supplier. The agreement may be a contract, a license, or a memorandum of agreement (MOA). The agreement is legally binding. Performance measures against the agreement are typically created and documented in a service level agreement (SLA), a secondary agreement that often supports the legal agreement.

Appraisal scope
The part of the organization that is the focus of a CERT-RMM-based appraisal of current resilience practices. The scope of an appraisal is typically, but not necessarily, the same as the scope of the improvement effort. (See related glossary terms "model scope" and "organizational scope.")

Area of impact or organizational impact area
Areas in which criteria are established to determine and express the potential impact of realized risk on the organization. Typical areas of impact include life and safety of employees and customers, financial, legal, and productivity. [RISK]

Asset or organizational asset
Something of value to the organization; typically, people, information, technology, and facilities that high-value services rely on. [ADM]

Asset custodian
A person or organizational unit, internal or external to the organization, responsible for satisfying the resilience requirements of a high-value asset while it is in their care. For example, a system administrator on a server that contains the vendor database would be a custodian of that asset. [ADM] [RRM]

Asset Definition and Management (ADM)
An engineering process area in CERT-RMM. The purpose of Asset Definition and Management is to identify, document, and manage organizational assets during their life cycle to ensure sustained productivity to support organizational services.

Asset disposition
The retirement of an asset from service, particularly information assets, commensurate with resilience requirements and information categorization and in accordance with any applicable rules, laws, and regulations. [KIM]

Asset inventory
An inventory (or inventories) of organizational assets—people, information, technology, and facilities. [ADM]

Asset-level resilience requirements
Asset-specific requirements that are set by the owners of the asset and are intended to establish the asset's protection and continuity needs with respect to its role in supporting mission assurance of a high-value service. [RRD]

Asset life cycle
The phases of an asset's life from development or acquisition to deployment to disposition. [ADM]

Asset owner
A person or organizational unit, internal or external to the organization, that has primary responsibility for the viability, productivity, and resilience of an organizational asset. For example, the Accounts Payable department is the owner of the vendor database. [ADM] [RRM]

Asset profile
Documentation of specific information about an asset (typically an information asset) that establishes ownership, a common definition, and other characteristics of the asset, such as its value. [ADM]

Assurance case
A structured set of arguments and a corresponding body of evidence demonstrating that a system satisfies specific claims with respect to its security, safety, or reliability properties. [RTSE]

Attack pattern
A design pattern describing the techniques that attackers might use to break a software product. [RTSE]

Attack surface
The set of ways in which an attacker can enter and potentially cause damage to a system. The larger the attack surface, the more insecure the system [http://www.cs.cmu.edu/~pratyus/as.html]. [RTSE]

Availability
For an asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed. [EC] [KIM] [PM]

Awareness
Focusing the attention of, creating cognizance in, and acculturating people throughout the organization to resilience issues, concerns, policies, plans, and practices. [OTA]

Awareness activity
A means for implementing the awareness approaches that the organization has considered and developed to meet the specific needs of the stakeholder community. Formal awareness training sessions, newsletters, email messages, and posters and other signage are examples of awareness activities. [OTA]

Awareness training
A means by which the organization can highlight important behaviors and begin the process of acculturating staff and business partners to important organizational resilience goals, objectives, and critical success factors. [OTA]

Awareness training waiver
See "waiver." [OTA]

Base measures
Data obtained by direct measurement. For example, the number of service continuity plans updated in the last 12 months is a base measure. [MA]

Baseline configuration item
A configuration item that serves as the baseline foundation for managing the integrity of the asset as it changes over its life cycle. [TM]

Business process
A series of discrete activities or tasks that contribute to the fulfillment of a service mission. (See related glossary term "service.")

Business requirement
A requirement that must be met to achieve business objectives. Such requirements establish the baseline for how organizational assets are used to support business processes. [ADM]

Capability level
An indicator of achievement of process capability in a process area. A capability level is achieved by visibly and verifiably implementing the required components of a process area. (See related glossary terms "required component" and "process area.")

Capacity planning
The process of determining the operational demand for a technology asset over a widely variable range of operational needs. [TM]

Change control or change management
A continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption. [RRM] [TM] [KIM]

Collocation (also co-location or colocation)
The act or result of placing or arranging together. In facilities management, collocation refers to the grouping of facilities, the effects of which must be considered in service continuity planning. [EC]

Communications (COMM)
An enterprise process area in CERT-RMM. The purpose of Communications is to develop, deploy, and manage internal and external communications to support resilience activities and processes.

Communications stakeholder
A person or group that has a vested interest in being involved in or a beneficiary of the organization's resilience communications activities. [COMM]

Compliance (COMP)
An enterprise process area in CERT-RMM. The purpose of Compliance Management is to ensure awareness of and compliance with an established set of relevant internal and external guidelines, standards, practices, policies, regulations, and legislation, and other obligations (such as contracts and service level agreements) related to managing operational resilience.

Compliance
A process that characterizes the activities that the organization performs to identify the internal and external guidelines, standards, practices, policies, regulations, and legislation to which they are subject and to comply with these obligations in an orderly, systematic, efficient, timely, and accurate manner. [COMP]

Compliance knowledgebase
A common accessible information repository for compliance data. The repository may include documentation of the compliance obligations and their owners and due dates, the results of compliance and substantive testing of controls, compliance targets and metrics, compliance reports, non-compliance reports, remediation plans, and tracking data to provide status on satisfying compliance obligations. [COMP]

Compliance obligations
The internal and external guidelines, standards, practices, policies, regulations, and legislation that the organization has an obligation to comply with. [COMP]

Condition
A term that collectively describes a vulnerability, an actor, a motive, and an undesirable outcome. A condition is essentially a threat that the organization must identify and analyze to determine if exploitation of the threat could result in undesirable consequences. [RISK] (See related glossary term "consequence.")

Confidentiality
For an asset, the quality of being accessible only to authorized people, processes, and devices. [KIM]

Configuration item
An asset or a series of related assets (typically information or technology-focused) that are placed under configuration management processes. [KIM] [TM]

Configuration management
A process for managing the integrity of an information or technology asset over its lifetime. Typically includes change control processes. [KIM] [TM]

Consequence
The unwanted effect, undesirable outcome, or impact to the organization as the result of exploitation of a condition or threat. [RISK] (See related glossary term "condition.")

Constellation
In the CMMI architecture, a collection of components that are used to construct models, training materials, and appraisal materials in an area of interest (e.g., services and development).

Container (information asset container)
A physical or logical location where assets are stored, transported, and processed. A container can encompass technical containers (servers, network segments, personal computers), physical containers (paper, file rooms, storage spaces, or other media such as CDs, disks, and flash drives), and people (including people who might have detailed knowledge about the information asset). [KIM]

Continuity of operations
An organization's ability to sustain assets and services in light of realized risk. Typically used interchangeably with service continuity. [RISK] [SC] (See related glossary term "Service Continuity.")

Controls
The methods, policies, and procedures—manual or automated—that are adopted by an organization to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, the promotion of administrative efficiency, and adherence to standards. [CTRL] [KIM]

Controls Management (CTRL)
An engineering process area in CERT-RMM. The purpose of Controls Management is to establish, implement, monitor, and manage an internal control system that ensures the effectiveness and efficiency of operations through mission assurance of high-value services.

Convergence
The harmonization of operational risk management activities that have similar objectives and outcomes.

Corrective maintenance
A process of correcting and repairing problems that degrade the operational capability of facility services. [EC]

Cost of resilience
An accumulation of expense and capital costs related to providing resilience services and achieving resilience requirements. [FRM]

Credentialing
A process for identifying, acquiring, and maintaining access for first responders (vital staff members) from governmental authorities. [PM]

Crisis
An incident in which the impact to the organization is imminent or immediate. A crisis requires immediate organizational action because the effect of the incident is already felt by the organization and must be limited or contained. [IMC]

Critical success factors
The key areas in which favorable results are necessary to achieve goals. They are both internal and external to the organization. They can originate in the organization's particular industry and with its peers, in its operating environment, from temporary barriers, challenges, or problems, or from the various domains of organizational management. [RRD]

Cross-training
Training in different roles or responsibilities within the organization, thus preparing staff to accept and perform new roles, however temporary, until a return to business as usual can be accomplished. [PM]

Cryptographic controls
Encryption of data and information that provides an additional layer of control over information assets by ensuring that access is limited to those who have the appropriate deciphering keys. [KIM]

Custodian
See "asset custodian."

Defined process
A managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines; has a maintained process description; and contributes work products, measures, and other process improvement information to organizational process assets. [OPD] (See related glossary terms "managed process" and "organization's set of standard processes.")

Deprovisioning
The process of revoking or removing an identity's access to organizational assets. [AM] (See related glossary term "provisioning.")

Derived measures
Data obtained by combining two or more base measures. For example, the percentage of risk mitigation plans completed on time in the last 12 months. [MA]

Disposition
The appropriate and proper retirement of an asset at the end of its useful life. [KIM] [RISK]

Encryption policies
Policies that govern the use of cryptographic technologies as appropriate or required for each level of information asset categorization. Includes organizational policies that manage the assignment of use, storage, disposal, and protection of cryptographic keys (such as public and private keys). [KIM]

Enterprise
Synonymous with "organization."

Enterprise Focus (EF)
An enterprise process area in CERT-RMM. The purpose of Enterprise Focus is to establish sponsorship, strategic planning, and governance over the operational resilience management process.

Enterprise-level resilience requirement
Resilience requirements that reflect enterprise-level needs, expectations, and constraints. These requirements affect nearly all aspects of an organization's operations. [RRD]

Environmental Control (EC)
An operations process area in CERT-RMM. The purpose of Environmental Control is to establish and manage an appropriate level of physical, environmental, and geographical controls to support the resilient operations of services in organizational facilities.

Establish and maintain
Whenever "establish and maintain" is used in a specific practice, it refers not only to the development and maintenance of the object of the practice (such as a policy) but to the documentation of the object and observable usage of the object. For example, "Establish and maintain an organizational policy for planning and performing the organizational process focus process" means that not only must a policy be formulated, but it also must be documented, and it must be used throughout the organization.

Event
One or more occurrences that affect organizational assets and have the potential to disrupt operations. [IMC] (See related glossary term "incident.")

Event triage
The process of categorizing, correlating, and prioritizing events with the objective of assigning events to incident handling and response. [IMC]

Exercise
The testing of a service continuity plan on a regular basis to ensure that it will achieve its stated objectives when executed as the result of a disruption or interruption. [SC]

Expected component
A model component that explains what may be done to satisfy a required CERT-RMM component. Specific and generic practices are expected model components. Model users can implement the expected components explicitly or implement equivalent alternative practices. (See related glossary terms "informative component" and "required component.")

External Dependencies Management (EXD)
An operations process area in CERT-RMM. The purpose of External Dependencies Management is to establish and manage an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities.

External dependency
An external dependency exists when an external entity has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to one or more assets or services of the organization. [EXD] (See related glossary term "external entity.")

External entity
An individual, business, or business unit (such as a customer, a contractor, or another group within the same enterprise) that is external to and in a supporting or influencing relationship with the organization that is using a process area. [EXD]

Facility
Any tangible and physical asset that is part of the organization's physical plant. Facilities include office buildings, warehouses, data centers, and other physical structures. [ADM] [EC]

Federation
The assembled identity of an object across organizational units, organizations, systems, or other domains where the object has multiple identities. [ID]

Financial Resource Management (FRM)
An enterprise process area in CERT-RMM. The purpose of Financial Resource Management is to request, receive, manage, and apply financial resources to support resilience objectives and requirements.

First responder
Vital staff trained to conduct damage assessment after a disruption and recommend a path to re-establishing the high-value services of the organization. [PM]

Functional monitoring requirements
Requirements that describe, at a detailed level, what must be performed to meet the monitoring requirement. Specific infrastructure needs are a type of functional monitoring requirement. [MON]

Fuzz testing
A means of testing that causes a software program to consume deliberately malformed data to see how the program reacts [Microsoft 2009]. [RTSE]

Generic goal
A required model component that describes characteristics that must be present to institutionalize processes that implement a process area. (See related glossary term "institutionalization.")

Generic practice
An expected model component that is considered important in achieving the associated generic goal. The generic practices associated with a generic goal describe the activities that are expected to result in achievement of the generic goal and contribute to the institutionalization of the processes associated with a process area.

Generic practice elaboration
An informative model component that appears after a generic practice to provide guidance on how the generic practice should be applied to the process area.

Geographical dispersion
The specific and planned dispersion or scattering of physical structures and facilities so that they are not all affected by a single event or incident. [EC]

Governance
An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. [EF]

High-value assets
People, information, technology, or facilities on whose availability, confidentiality, integrity, and productivity a high-value service is dependent. [ADM]

High-value services
Services on which the success of the organization's mission depends. [RRD] [EF]

Human Resource Management (HRM)
An enterprise process area in CERT-RMM. The purpose of Human Resource Management is to manage the employment life cycle and performance of staff in a manner that contributes to the organization's ability to manage operational resilience.

Identity
Documentation of certain information about a person, object, or entity that may require access to organizational assets to fulfill its role in executing services. [ID]

Identity community
Defines the baseline population of persons, objects, and entities—internal and external to the organization—that could be or are authorized to access and use organizational assets commensurate with their job responsibilities and roles. Also, the collection of the organization's identity profiles. [ID]

Identity Management (ID)
An operations process area in CERT-RMM. The purpose of Identity Management is to create, maintain, and deactivate identities and associated attributes that provide access to organizational assets.

Identity management
A process that addresses the management of the life cycle of objects (typically people, but often systems, devices, or other processes) that need some level of trusted access to organizational assets. [ID]

Identity profile
Documentation of all of the relevant information necessary to describe the unique attributes, roles, and responsibilities of the associated person, object, or entity. [ID]

Identity registration
The process of making an identity "known" to the organization as a person, object, or entity that may require access to organizational assets and that may need to be authenticated and authorized to use access privileges. [ID]

Identity repository
A common accessible information repository that provides a single (or virtual) consistent source of information about organizational identities. [ID]

Impact valuation
Determines the extent of the impact of operational risk using the organization's risk measurement criteria. [RISK]

Incident
An event (or series of events) of higher magnitude that significantly affects organizational assets and requires the organization to respond in some way to prevent or limit organizational impact. [IMC]

Incident closure
The retirement of an incident that has been responded to (i.e., there are no further actions required, and the organization is satisfied with the result) and for which the organization has performed a formal post-incident review. [IMC]

Incident escalation
The process of notifying relevant stakeholders about an incident that requires an organizational response and involves stakeholder actions to implement, manage, and bring to closure with an appropriate and timely solution. [IMC]

Incident life cycle
The life cycle of an incident from detection to closure. Collectively, the processes of logging, tracking, documenting, escalating and notifying, gathering and preserving evidence, and closing incidents. [IMC]

Incident Management and Control (IMC)
An operations process area in CERT-RMM. The purpose of Incident Management and Control is to establish processes to identify and analyze events, detect incidents, and determine an appropriate organizational response.

Incident owner
The individuals or teams to whom an incident is assigned for containment, analysis, and response. [IMC]

Incident response
The actions the organization takes to prevent or contain the impact of an incident to the organization while it is occurring or shortly after it has occurred. [IMC]

Incident stakeholder
A person or organization that has a vested interest in the management of an incident throughout its life cycle. [IMC]

Information asset
Information or data that is of value to the organization, including diverse information such as patient records, intellectual property, customer information, and contracts. [ADM] [KIM]

Information asset baseline
A foundational configuration of an information asset from which changes to the asset can be detected over its life cycle. [KIM]

Information asset categorization
A process for labeling and handling the sensitivity of information assets, typically based on a categorization taxonomy or scheme. [KIM]

Information asset container
A technical or physical asset or a person in or on which information is stored, transported, or processed. [ADM] [KIM]

Information asset owner
See related glossary term "asset owner." [ADM]

Informative component
A model component that helps model users understand required and expected components. (See related glossary terms "expected component" and "required component.")

Informative components can contain examples, detailed explanations, or other helpful information. Subpractices, notes, references, goal titles, practice titles, sources, typical work products, amplifications, and generic practice elaborations are informative model components.

Institutionalization
Incorporation into the ingrained way of doing business that an organization follows routinely as part of its corporate culture.

Integrity
For an asset, the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner. [KIM] [TM]

Intellectual property
The unique information assets of the organization that are created by the organization and are vital to its success. Intellectual property may include trade secrets, formulas, trademarks, and other organizationally produced assets. [KIM]

Internal control system
The methods, policies, and procedures used to protect and sustain high-value assets at a level commensurate with their role in supporting organizational services. [KIM] (See related glossary term "high-value assets.")

Key control indicators
Organizationally specific indicators that provide information about the effectiveness of the organization's internal control system. [EF]

Key performance indicators
Organizationally specific performance metrics that measure progress against the organization's strategic objectives and critical success factors. [EF]

Key risk indicators
Organizationally specific thresholds that, when crossed, indicate levels of risk that may be outside of the organization's risk tolerance. [EF] [RISK]

Knowledge and Information Management (KIM)
An operations process area in CERT-RMM. The purpose of Knowledge and Information Management is to establish and manage an appropriate level of controls to support the confidentiality, integrity, and availability of the organization's information, vital records, and intellectual property.

Line of business
A logical grouping of organizational units that have a common purpose, such as production of products for a particular market segment.

Managed process
A performed process that is planned and executed in accordance with policy; employs skilled people having adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled, and reviewed; and is evaluated for adherence to its process description. (See related glossary term "performed process.")

Measurement and Analysis (MA)
A process management process area in CERT-RMM. The purpose of Measurement and Analysis is to develop and sustain a measurement capability that is used to support management information needs for managing the operational resilience management process.

Measurement objectives
Documents the purpose for which measurements and analysis are done and specifies the kinds of actions that may be taken based on the results of data analysis. [MA]

Measures
Measurements of the resilience process that may be categorized by obtaining direct measurements (base measures) or by obtaining measurements that are a combination of two or more base measures (derived measures). [MA]

Misuse/abuse case
A descriptive statement of the undesirable, nonstandard conditions that software is likely to face during its operation from either unintentional misuse or intentional and malicious misuse or abuse. [RTSE]

Model scope
The parts of CERT-RMM that will be used to guide the improvement effort.

Monitoring (MON)
A process management process area in CERT-RMM. The purpose of Monitoring is to collect, record, and distribute information about the operational resilience management process to the organization on a timely basis.

Monitoring infrastructure
The technologies and support services that are needed to support the achievement of monitoring requirements. [MON]

Monitoring requirements
The requirements established to determine the information gathering and dissemination needs of stakeholders. [MON]

Monitoring stakeholder
A person or group that has a vested interest in being involved in or a beneficiary of the organization's monitoring activities. [MON]

Operational constraint
A limit imposed on an organization's operational activities. These limits can be imposed by the organization on itself or can come from the organization's operating environment (e.g., regulations). [RRD]

Operational resilience
The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk. (See related glossary term "operational risk.")

Operational resilience management
The processes by which an organization designs, develops, implements, manages, and improves strategies for protecting and sustaining high-value services and associated assets such as people, information, technology, and facilities.

Operational resilience requirements
Refers collectively to requirements that ensure the protection of high-value assets as well as their continuity when a disruptive event has occurred. The requirements traditionally encompass security, business continuity, and IT operational requirements. These include the security objectives for information assets (confidentiality, integrity, and availability) as well as the requirements for business continuity planning and recovery and the availability and support requirements of the organization's technical infrastructure. [RRD]

Operational risk
The potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events.

Operational risk taxonomy
The collection and cataloging of common operational risks that the organization is subjected to and must manage. The risk taxonomy is a means for communicating these risks and for developing organizational unit and line of business-specific mitigation actions if operational assets and services are affected by them. [RISK]

Organization
An administrative structure in which people collectively manage one or more services as a whole, and whose services share a senior manager and operate under the same policies. May consist of many organizations in many locations with different customers. (See related glossary terms "enterprise" and "organizational unit.")

Organization's process asset library
A library of information used to store and make available process assets that are useful to those who are defining, implementing, and managing processes in the organization. This library contains process assets that include process-related documentation such as policies, defined processes, checklists, lessons-learned documents, templates, standards, procedures, plans, and training materials.

Organization's set of standard processes
A collection of definitions of the processes that guide activities in an organization. These process descriptions cover the fundamental process elements (and their relationships to each other, such as ordering and interfaces) that must be incorporated into the defined processes that are implemented in projects across the organization. A standard process enables consistent development and maintenance activities across the organization and is essential for long-term stability and improvement. [OPD] (See related glossary terms "defined process" and "process element.")

Organizational asset
See "asset."

Organizational impact area
See "area of impact."

Organizational process assets
Artifacts that relate to describing, implementing, and improving processes (e.g., policies, measurements, process descriptions, and process implementation support tools). The term *process assets* is used to indicate that these artifacts are developed or acquired to meet the business objectives of the organization, and they represent investments by the organization that are expected to provide current and future business value. (See related glossary term "process asset library.")

Organizational Process Definition (OPD)
A process management process area in CERT-RMM. The purpose of Organizational Process Definition is to establish and maintain a usable set of organizational process assets and work environment standards for operational resilience.

Organizational Process Focus (OPF)
A process management process area in CERT-RMM. The purpose of Organizational Process Focus is to plan, implement, and deploy organizational process improvements based on a thorough understanding of current strengths and weaknesses of the organization's operational resilience processes and process assets.

Organizational process maturity
In models with a staged representation, organizational process maturity is measured by the degree of process improvement across predefined sets of process areas. Since CERT-RMM does not have a staged representation, characterization of organizational process maturity can only be implied by reaching successively higher levels of capability across CERT-RMM process areas.

Organizational scope
The part of the organization that is the focus of the CERT-RMM deployment.

Organizational sensitivity
The degree to which access to an information asset must be limited due to confidentiality or privacy requirements. [ADM]

Organizational Training and Awareness (OTA)
An enterprise process area in CERT-RMM. The purpose of Organizational Training and Awareness is to promote awareness and develop skills and knowledge of people in support of their roles in attaining and sustaining operational resilience.

Organizational subunit
Any sub-element of the organizational unit. An organizational subunit is fully contained within the organizational unit.

Organizational superunit
Any part of the organization that is at a higher level than the organizational unit. Organizational superunit can also be used to refer to the entire organization.

Organizational unit
A distinct subset of an organization or enterprise. An organizational unit is typically part of a larger organization, although in a small organization the organizational unit may be the whole organization.

Organizationally high-value services
Services on which the success of the organization's mission is dependent. [RRD] [EF]

People
All staff, both internal and external to the organization, and all managers employed in some manner by the organization to perform a role or fulfill a responsibility that contributes to meeting the organization's goals and objectives. [PM]

People Management (PM)
An operations process area in CERT-RMM. The purpose of People Management is to establish and manage the contributions and availability of people to support the resilient operation of organizational services.

Perfective maintenance
Maintenance performed by acquiring additional or improved operational capacity. [EC]

Performed process
A process that accomplishes the needed work to produce work products. The specific goals of the process area are satisfied.

Physical control
A type of control that prevents physical access to and modification of information assets or physical access to technology and facilities. Physical controls often include such artifacts as card readers and physical barrier methods. [KIM] [TM] [EC]

Planned downtime
Acceptable and planned interruption of the availability of an information or technology asset, usually as the result of a user- or management-initiated event. [TM]

Post-incident review
A formal part of the incident closure process that refers to the organization's formal examination of the causes of an incident and the ways in which the organization responded to it, as well as the administrative, technical, and physical control weaknesses that may have allowed the incident to occur. [IMC]

Preventive maintenance
Pre-planned activities performed to prevent potential facility problems from occurring. [EC]

Privacy
The assurance that information about an individual is disclosed only to people, processes, and devices authorized by that individual or permitted under privacy laws and regulations. [KIM]

Privilege
See "access privilege." [AM]

Problem management
The process that an organization uses to identify recurring problems, examine root causes, and develop solutions for these problems to prevent future, similar incidents. [IMC]

Process
Activities that can be recognized as implementations of practices in the model. These activities can be mapped to one or more practices in process areas to allow the model to be useful for process improvement and process appraisal. (See related glossary terms "process area," "subprocess," and "process element.")

There is a special use of the phrase "the process" in the statements and descriptions of the generic goals and generic practices. In that context, "the process" is the process or processes that implement the process area.

Process architecture
The ordering, interfaces, interdependencies, and other relationships among the process elements in a standard process. Process architecture also describes the interfaces, interdependencies, and other relationships between process elements and external processes (e.g., contract management). [OPD]

Process area
A cluster of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making improvement in that area.

Process asset library
A collection of process asset holdings that can be used by an organization or project. (See related glossary term "organization's process asset library.")

Process capability
The range of expected results that can be achieved by following a process. The generic goals and practices define the degree to which a process is institutionalized; capability levels indicate the degree to which a process is institutionalized.

Process element
The fundamental unit of a process. A process can be defined in terms of subprocesses or process elements. A subprocess can be further decomposed into subprocesses or process elements; a process element cannot. (See related glossary term "subprocess.")

Each process element covers a closely related set of activities (e.g., estimating element, peer review element). Process elements can be portrayed using templates to be completed, abstractions to be refined, or descriptions to be modified or used. A process element can be an activity or a task. [OPD]

Process performance
A measure of actual results achieved by following a process. It is characterized by both process measures (e.g., vulnerabilities eliminated before being exploited) and product or service measures (e.g., control system network unavailability due to exploited vulnerabilities).

Protection strategy
The strategy, related controls, and activities necessary to protect an asset from undesired harm or disruptive events. The protection strategy is relative to the conditions to which the asset is subjected. (See related glossary term "condition.")

Provisioning
The process of assigning or activating an identity profile and its associated roles and access privileges. [ID]

Proximity
The relative distance between facilities, which is a consideration in collocation and geographical dispersion. [EC] (See related glossary terms “collocation” and “geographical dispersion.”)

Public infrastructure
Infrastructure owned by the community in the geographical area that contains a facility. Includes telecommunications and telephone services, electricity, natural gas, and other energy sources, water and sewer services, trash collection and disposal, and other support services. [EC]

Public services
Services that are provided in the community or in the geographical area that contains a facility. Includes fire response and rescue services, local and federal law enforcement, emergency management services such as paramedics and first responders, and animal control. [EC]

Recovery point objective (RPO)
Establishes the point to which an information or technology asset (typically an application system) must be restored to allow recovery of the asset and associated services after a disruption. [TM]

Recovery time objective (RTO)
Establishes the period of acceptable downtime of an information or technology asset after which the organization would suffer an unwanted consequence or impact. [TM]

Regulation
A type of compliance obligation issued by a governmental, regulatory, or other agency. [COMP]

Release build
A version of an information or technology asset that is to be released into production; an object in the release management process. [KIM] [TM]

Release management
The process of managing successive release of versions of information and technology assets into an operations and production environment. [KIM] [TM]

Required component
A CERT-RMM component that is essential to achieving process improvement in a given process area. Required components are used in appraisals to determine process capability. Specific goals and generic goals are required components. (See related glossary terms “expected component” and “informative component.”)

Residual risk
The risk that remains and is accepted by the organization after mitigation plans are implemented. [RISK]

Resilience budget
A budget specifically developed and funded to support the organization's resilience activities. [FRM]

Resilience management
See "operational resilience management."

Resilience obligations
An understanding of a commitment, promise, or duty to follow and enforce the resilience requirements of the organization. [HRM]

Resilience requirement
A constraint that the organization places on the productive capability of an asset to ensure that it remains viable and sustainable when charged into production to support a service.

Resilience Requirements Development (RRD)
An engineering process area in CERT-RMM. The purpose of Resilience Requirements Development is to identify, document, and analyze the operational resilience requirements for high-value services and related assets.

Resilience Requirements Management (RRM)
An engineering process area in CERT-RMM. The purpose of Resilience Requirements Management is to manage the resilience requirements of high-value services and associated assets and to identify inconsistencies between these requirements and the activities that the organization performs to meet the requirements.

Resilience specifications
Criteria that the organization establishes for a working relationship with an external entity, which may be incorporated into contractual terms. Typically include the resilience requirements of any of the organization's high-value assets and services that are placed in the external entity's control. Also may include required characteristics of the external entity (e.g., financial condition and experience), required behaviors of the external entity (e.g., security and training practices), and performance parameters that must be exhibited by the external entity (e.g., recovery time after an incident and response time to service calls).

Resilience staff
Internal or external staff who are specifically involved in or assigned to resilience-focused activities that are typically found in security, business continuity, and IT operations disciplines. [OTA]

Resilience training
The process and activities focused on imparting the necessary skills and knowledge to people for performing their roles and responsibilities in support of the organization's operational resilience management process. [OTA]

Resilience training needs
Training requirements related to the skills and competencies required at a tactical level to carry out the activities required for managing operational resilience. [OTA]

Resilient Technical Solution Engineering (RTSE)
An engineering process area in CERT-RMM. The purpose of Resilient Technical Solution Engineering is to ensure that software and systems are developed to satisfy their resilience requirements.

Return on resilience investment (RORI)
The return on investment for funding resilience activities. Provides a way to justify resilience costs and provides direct support for the contribution that managing operational resilience makes in achieving strategic objectives. [FRM]

Risk
The possibility of suffering harm or loss. From a resilience perspective, risk is the combination of a threat or vulnerability (condition) and the impact (consequence) to the organization if the threat or vulnerability is exploited. In CERT-RMM, this definition is typically applied to the asset or service level such that risk is the possibility of suffering harm or loss due to disruption of high-value assets and services. [RISK]

Risk analysis
A risk management process focused on understanding the condition and consequences of risk, prioritizing risks, and determining a path for addressing risks. Determines the importance of each identified operational risk and is used to facilitate the organization's risk disposition and mitigation activities. [RISK]

Risk appetite
An organization's stated level of risk aversion. Informs the development of risk evaluation criteria in areas of impact for the organization. [RISK] (See related glossary terms "area of impact," "risk measurement criteria," and "risk tolerance.")

Risk category
An organizationally defined description of risk that typically aligns with the various sources of operational risk but can be tailored to the organization's unique risk environment. Risk categories provide a means to collect and organize risks to assist in the analysis and mitigation processes. [RISK]

Risk disposition
A statement of the organization's intention for addressing an operational risk. Typically limited to accept, transfer, research, or mitigate. [RISK]

Risk Management (RISK)
An enterprise process area in CERT-RMM. The purpose of Risk Management is to identify, analyze, and mitigate risks to organizational assets that could adversely affect the operation and delivery of services.

Risk management
The continuous process of identifying, analyzing, and mitigating risks to organizational assets that could adversely affect the operation and delivery of services. [RISK]

Risk measurement criteria
Objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on areas of impact. [RISK] (See related glossary term "area of impact.")

Risk mitigation
The act of reducing risk to an acceptable level. [RISK]

Risk mitigation plan
A strategy for mitigating risk that seeks to minimize the risk to an acceptable level. [RISK]

Risk parameter (risk management parameter)
Organizationally specific risk tolerances used for consistent measurement of risk across the organization. Risk parameters include risk tolerances and risk measurement criteria. [RISK] (See related glossary terms "risk tolerance" and "risk measurement criteria.")

Risk statement
A statement that clearly articulates the context, conditions, and consequences of risk. [RISK]

Risk taxonomy
See "operational risk taxonomy."

Risk threshold
An organizationally developed type of risk parameter that is used by management to determine when a risk is in control or when it has exceeded acceptable organizational limits. [RISK]

Risk tolerance
Thresholds that reflect the organization's level of risk aversion by providing levels of acceptable risk in each operational risk category that the organization established. Risk tolerance, as a risk parameter, also establishes the organization's philosophy on risk management—how risks will be controlled, who has the authorization to accept risk on behalf of the organization, and how often and to what degree operational risk should be assessed. [RISK]

Root cause analysis
An approach for determining the underlying causes of events or problems as a means of addressing the symptoms of such events as they manifest in organizational disruptions. [VAR]

Scope
See "appraisal scope," "model scope," and "organizational scope."

Secure design pattern
A general, reusable solution to a commonly occurring problem in design. A design pattern is not a finished design that can be transformed directly into code. It is a description or template for how to solve a problem that can be used in many different situations.

Secure design patterns are meant to eliminate the accidental insertion of vulnerabilities into code or to mitigate the consequences of vulnerabilities. Secure design patterns address security issues at widely varying levels of specificity, ranging from architectural-level patterns involving the high-level design of the system down to implementation-level patterns providing guidance on how to implement portions of functions or methods in the system [Dougherty 2009]. [RTSE]

Sensitivity
A measure of the degree to which an information asset must be protected based on the consequences of its unauthorized access, modification, or disclosure. [KIM]

Service
A set of activities that the organization carries out in the performance of a duty or in the production of a product. [ADM] [EF] (See related glossary term "business process.")

Service Continuity (SC)
An engineering process area in CERT-RMM. The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

Service continuity plan (business continuity plan)
A service-specific plan for sustaining services and associated assets under degraded conditions. [SC]

Service level agreement (SLA)
A type of agreement that specifies levels of service expected from business partners in the performance of a contract or agreement. In CERT-RMM, SLAs are expanded to include the satisfaction of resilience requirements by business partners when one or more organizational assets are in their custodial care.

Service-level resilience requirements
Service requirements established by owners of the service such as an organizational unit or a line of business. [RRD] (See related glossary term "asset-level resilience requirements.")

Service profile
A profile that describes services in sufficient detail to capture the activities, tasks, and expected outcomes of the services and the assets that are vital to the service. [EF]

Service resilience requirements
Resilience needs of a service in its pursuit of its mission. Resilience requirements for services primarily address availability and recoverability but are also directly related to the confidentiality, integrity, and availability requirements of associated assets. [RRD]

Services map
Details the relationships between a service, associated business processes, and associated assets. [RRD]

Shared resilience requirements
Shared requirements are those that are developed for shared organizational assets such as a facility in which more than one high-value service is executed. [RRD]

Skills inventory or repository
A means for identifying and documenting the current skill set of the organization's human resources. [HRM]

Specific goal
A required model component that describes the unique characteristics that must be present to satisfy the process area. (See related glossary terms “process area” and “required component.”)

Specific practice
An expected model component that is considered important in achieving the associated specific goal. The specific practices describe the activities expected to result in achievement of the specific goals of a process area. (See related glossary terms “expected component,” “process area,” and “specific goal.”)

Staff
All people, both internal and external to the organization, employed in some manner by the organization to perform a role or fulfill a responsibility that contributes to meeting the organization’s goals and objectives. Does not include those in managerial roles.

Stakeholder
A person or organization that has a vested interest in the organization or its activities. (See related glossary terms “communications stakeholder” and “monitoring stakeholder.”)

Standard process
An operational definition of the basic process that guides the establishment of a common process in an organization. A standard process describes the fundamental process elements that are expected to be incorporated into any defined process. It also describes relationships (e.g., ordering, interfaces) among these process elements. [OPD] (See related glossary term “defined process.”)

Strategic objectives (strategic drivers)
Strategic objectives are the performance targets that the organization sets to accomplish its mission, vision, values, and purpose. [EF]

Strategic planning
The process of developing strategic objectives and plans for meeting these objectives. [EF]

Subprocess
A process that is part of a larger process. A subprocess can be decomposed into subprocesses or process elements. [OPD] (See related glossary terms “process” and “process element.”)

Succession planning
A form of continuity planning for vital staff and/or decision making management focused on providing a smooth transition for vital roles and sustaining the high-value services of the organization. [PM]

Supplier
An internal or external organization or contractor who supplies key products and services to the organization to contribute to accomplishing the missions of its high-value services.

Sustain
Maintain in a desired operational state.

Technical control
A type of technical mechanism that supports protection methods for assets such as firewalls and electronic access controls. [KIM] [TM]

Technology asset
Any hardware, software, or firmware used by the organization in the delivery of services. [TM]

Technology interoperability
The ability of technology assets to exist and operate in a connected manner to meet an organizational goal, objective, or mission. [TM]

Technology Management (TM)
An operations process area in CERT-RMM. The purpose of Technology Management is to establish and manage an appropriate level of controls related to the integrity and availability of technology assets to support the resilient operations of organizational services.

Threat
A situation, vulnerability, or condition that can be exploited to produce an unexpected or unwanted outcome for the organization. [RISK] [VAR]

Threat actor
A person or event that has the potential to exploit a threat. [VAR] [RISK]

Threat environment
The set of all types of threats that could affect the current operations of the organization. (See related glossary term “threat.”)

Threat motive
The reason that a threat actor would exploit a vulnerability or threat. [VAR] [RISK]

Unplanned downtime
Interruption in the availability of an information or technology asset (and in some cases, a facility asset) due to an unplanned event or incident, often resulting from diminished operational resilience. [TM]

User
Any entity or object that the organization has granted some form of access to an organizational asset. Typically referred to as an “identity.” (See related glossary term “identity.”)

Vital records
A record that must be preserved and available for retrieval if needed. This refers to records or documents that, for legal, regulatory, or operational reasons, cannot be irretrievably lost or damaged without materially impairing the organization’s ability to conduct business. [KIM]

Vital staff
A select group of individuals who are absolutely essential to the sustained operation of the organization, particularly under stressful conditions. [PM]

Vulnerability
A potential exposure or weakness that could be exploited. The susceptibility of an organizational service or asset to disruption. [VAR]

Vulnerability Analysis and Resolution (VAR)
An operations process area in CERT-RMM. The purpose of Vulnerability Analysis and Resolution is to identify, analyze, and manage vulnerabilities in an organization's operating environment.

Vulnerability management strategy
A strategy for identifying and reducing exposure to known vulnerabilities. [VAR]

Vulnerability repository
An organizational inventory of known vulnerabilities. [VAR]

Vulnerability resolution
The action that the organization takes to reduce or eliminate exposure to vulnerability. [VAR]

Waiver
Documentation for staff members who have been exempted from awareness training or other activities for any reason. Such documentation includes the rationale for the waiver and approval by the individual's manager (or similarly appropriate person). Each required course should include criteria for granting training waivers. [OTA]

Acronyms and Initialisms

ADM
Asset Definition and Management (process area)

AM
Access Management (process area)

BSIMM
Building Security In Maturity Model

CBCP
Certified Business Continuity Professional

CCB
configuration control board

CIO
chief information officer

CISA
Certified Information Systems Auditor

CISSP
Certified Information Systems Security Professional

CL
capability level

CMF
CMMI Model Foundation

CMMI
Capability Maturity Model Integration

CMMI-ACQ
CMMI for Acquisition

CMMI-DEV
CMMI for Development

CMMI-SVC
CMMI for Services

CobiT
Control Objectives for Information and related Technology

COMM
Communications (process area)

COMP
Compliance (process area)

COPPA
Children's Online Privacy Protection Act

COR
cost of resilience

COSO
Committee of Sponsoring Organizations of the Treadway Commission frameworks

COTS
commercial off-the-shelf

CPA
Certified Public Accountant

CSIRT
computer security incident response team

CTRL
Controls Management (process area)

CVE
Common Vulnerabilities and Exposures project

CXO
higher level managers (CEO, CSO, etc.)

DBA
database administrator

DoD
Department of Defense

DRII
Disaster Recovery Institute International

EC
Environmental Control (process area)

EF
Enterprise Focus (process area)

EUDPD
European Union Data Protection Directive

EXD
External Dependencies Management (process area)

FBI
U.S. Federal Bureau of Investigation

FERC
Federal Energy Regulatory Commission

FERPA
Family Educational Right to Privacy Act

FCRA
Fair Credit Reporting Act

FRM
Financial Resource Management (process area)

FSTC
Financial Services Technology Consortium

GG
generic goal

GLB
Gramm-Leach-Bliley Act

GP
generic practice

HIPAA
Health Insurance Portability and Accountability Act

HRM
Human Resource Management (process area)

HVAC
heating, ventilation, and air conditioning

ID
Identity Management (process area)

IIA
Institute of Internal Auditors

IMC
Incident Management and Control (process area)

ISACA
Information Systems Audit and Control Association

ISO
International Organization for Standardization

ISSA
Information Systems Security Association

IT
information technology

ITIL
Information Technology Infrastructure Library

KCI
key control indicators

KIM
Knowledge and Information Management (process area)

KPI
key performance indicators

KRI
key risk indicators

MA
Measurement and Analysis (process area)

MCSE
Microsoft Certified Systems Engineer

MON
Monitoring (process area)

NFPA
National Fire Protection Association

OCTAVE
Operationally Critical Threat, Asset, and Vulnerability Evaluation

OPD
Organizational Process Definition (process area)

OPF
Organizational Process Focus (process area)

ORPG
operational resilience process group

OTA
Organizational Training and Awareness (process area)

OWASP
Open Web Applications Security Project

PA
process area

PCI DSS
Payment Card Industry Data Security Standard

PDA
personal digital assistant

PM
People Management (process area)

RFP
request for proposals

RFID
radio frequency identification

RISK
Risk Management (process area)

RMA
Risk Management Association

RMM
Resilience Management Model

RORI
return on resilience investment

RPO
recovery point objective

RRD
Resilience Requirements Development (process area)

RRM
Resilience Requirements Management (process area)

RTO
recovery time objective

RTSE
Resilient Technical Solution Engineering (process area)

SAMM
Software Assurance Maturity Model

SC
Service Continuity (process area)

SCADA
supervisory control and data acquisition

SCAMPI
Standard CMMI Appraisal Method for Process Improvement

SEI
Software Engineering Institute

SG
specific goal

SLA
service level agreement

SOX
Sarbanes-Oxley Act

SP
specific practice

TM
Technology Management (process area)

US-CERT
United States Computer Emergency Readiness Team

VAR
Vulnerability Analysis and Resolution (process area)

References

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

[Allen 2004]
Allen, J.; et al. *Best in Class Security and Operations Roundtable Report* (CMU/SEI-2004-SR-002). Software Engineering Institute, Carnegie Mellon University, 2004. Available upon request from info@sei.cmu.edu.

[Alberts 1999]
Alberts, C. J.; Behrens, S. G.; Pethia, R. D., & Wilson, W. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0* (CMU/SEI-99-TR-017). Software Engineering Institute, Carnegie Mellon University, 1999. http://www.sei.cmu.edu/library/abstracts/reports/99tr017.cfm

[Caralli 2004]
Caralli, R. A. *Managing for Enterprise Security* (CMU/SEI-2004-TN-046). Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/library/abstracts/reports/04tn046.cfm

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

[Caralli 2007]
Caralli, R. A.; et al. *Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes* (CMU/SEI-2007-TR-009). Software Engineering Institute, Carnegie Mellon University, 2007. http://www.sei.cmu.edu/library/abstracts/reports/07tr009.cfm

[CMMI Product Team 2006]
CMMI Product Team. *CMMI for Development, Version 1.2* (CMU/SEI-2006-TR-008). Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu/library/abstracts/reports/06tr008.cfm

[CMMI Product Team 2009]
CMMI Product Team. *CMMI for Services, Version 1.2* (CMU/SEI-2009-TR-001). Software Engineering Institute, Carnegie Mellon University, 2009. http://www.sei.cmu.edu/library/abstracts/reports/09tr001.cfm

[Deming 2000]
Deming, W. E. *Out of the Crisis*. MIT Press, 2000.

[Dougherty 2009]
Dougherty, C.; Sayre, K., Seacord, R. C.; Svoboda, D.; & Togashi, K. *Secure Design Patterns* (CMU/SEI-2009-TR-010). Software Engineering Institute, Carnegie Mellon University, 2009. http://www.sei.cmu.edu/library/abstracts/reports/09tr010.cfm

[FFIEC 2004]
Federal Financial Institutions Examination Council. "Outsourcing Technology Services IT Examination Handbook," *Federal Financial Institutions Examination Council Handbook,* 2004. http://www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf

[Imai 1986]
Imai, M. *Kaizen: The Key to Japan's Competitive Success.* McGraw-Hill/Irwin, 1986.

[McFeeley 1996]
McFeeley, R. *IDEAL: A Users Guide for Software Process Improvement* (CMU/SEI-96-HB-001). Software Engineering Institute, Carnegie Mellon University, 1996. http://www.sei.cmu.edu/library/abstracts/reports/96hb001.cfm. See also: http://www.sei.cmu.edu/library/abstracts/presentations/idealmodelported.cfm

[Microsoft 2009]
Microsoft Corporation. *Microsoft Security Development Life Cycle, Version 4.1.* Microsoft Corporation, 2009. http://www.microsoft.com/security/sdl/

[REF Team 2008a]
Resiliency Engineering Framework Team. *CERT Resiliency Engineering Framework.* Software Engineering Institute, Carnegie Mellon University, 2008. http://www.cert.org/resilience/rmm_materials.html

[REF Team 2008b]
Resiliency Engineering Framework Team. *CERT Resiliency Engineering Framework: Code of Practice Crosswalk, Preview Version, v0.95R*. Software Engineering Institute, Carnegie Mellon University, 2008. http://www.cert.org/resilience/rmm_materials.html

[SCAMPI Upgrade Team 2006]
SCAMPI Upgrade Team. *Appraisal Requirements for CMMI, Version 1.2 (ARC, V1.2)* (CMU/SEI-2006-TR-011). Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu/library/abstracts/reports/06tr011.cfm. See also http://www.sei.cmu.edu/cmmi/tools/appraisals/materials.cfm

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	May 2010	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
CERT® Resilience Management Model, Version 1.0	FA8721-05-C-0003

6. AUTHOR(S)

Richard A. Caralli, Julia H. Allen, Pamela D. Curtis, David W. White, & Lisa R. Young

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2010-TR-012

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-2010-012

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

Organizations in every sector—industry, government, and academia—are facing increasingly complex operational environments and dynamic risk environments. These demands conspire to force organizations to rethink how they manage operational risk and the resilience of critical business processes and services.

The CERT® Resilience Management Model (CERT®-RMM) is an innovative and transformative way to approach the challenge of managing operational resilience in complex, risk-evolving environments. It is the result of years of research into the ways that organizations manage the security and survivability of the assets that ensure mission success. It incorporates concepts from an established process improvement community to allow organizations to holistically mature their security, business continuity, and IT operations management capabilities and improve predictability and success in sustaining operations whenever disruption occurs.

This report describes the model's key concepts, components, and process area relationships and provides guidance for applying the model to meet process improvement and other objectives. One process area is included in its entirety; the others are presented in outline form. All of the CERT-RMM process areas are available for download at www.cert.org/resilience.

14. SUBJECT TERMS	15. NUMBER OF PAGES
enterprise security management, strategic planning, information security, risk management, operational risk management, process improvement, resilience, operational resilience, capability model	258

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