CERT® Resilience Management Model
A Maturity Model for Managing Operational Resilience

Richard A. Caralli
Julia H. Allen
David W. White
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF FIGURES</td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xiii</td>
</tr>
<tr>
<td>PREFACE</td>
<td>xv</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>xxi</td>
</tr>
</tbody>
</table>

## PART ONE—ABOUT THE CERT RESILIENCE MANAGEMENT MODEL

### 1 INTRODUCTION

1.1 The Influence of Process Improvement and Capability Maturity Models 8
1.2 The Evolution of CERT-RMM 10
1.3 CERT-RMM and CMMI Models 15
1.4 Why CERT-RMM Is Not a *Capability Maturity* Model 18

### 2 UNDERSTANDING KEY CONCEPTS IN CERT-RMM

2.1 Foundational Concepts
   2.1.1 Disruption and Stress 21
   2.1.2 Convergence 23
   2.1.3 Managing Operational Resilience 25
2.2 Elements of Operational Resilience Management
   2.2.1 Services 27
   2.2.2 Business Processes 29
PART TWO—PROCESS INSTITUTIONALIZATION AND IMPROVEMENT 65

5 INSTITUTIONALIZING OPERATIONAL RESILIENCE MANAGEMENT PROCESSES 67

5.1 Overview 67

5.2 Understanding Capability Levels 68

5.3 Connecting Capability Levels to Process Institutionalization 69

5.3.1 Capability Level 0: Incomplete 70

5.3.2 Capability Level 1: Performed 70

5.3.3 Capability Level 2: Managed 70

5.3.4 Capability Level 3: Defined 72

5.3.5 Other Capability Levels 72

5.4 CERT-RMM Generic Goals and Practices 73

5.4.1 CERT-RMM Elaborated Generic Goals and Practices 74

5.5 Applying Generic Practices 74

5.6 Process Areas That Support Generic Practices 74

6 USING CERT-RMM 77

6.1 Examples of CERT-RMM Uses 78

6.1.1 Supporting Strategic and Operational Objectives 78

6.1.2 A Basis for Evaluation, Guidance, and Comparison 78

6.1.3 An Organizing Structure for Deployed Practices 79

6.1.4 Model-Based Process Improvement 80

6.2 Focusing CERT-RMM on Model-Based Process Improvement 80

6.2.1 Making the Business Case 81

6.2.2 A Process Improvement Process 82

6.3 Setting and Communicating Objectives Using CERT-RMM 83

6.3.1 Organizational Scope 85

6.3.2 Model Scope 87

6.3.3 Capability Level Targets 90

6.4 Diagnosing Based on CERT-RMM 92

6.4.1 Formal Diagnosis Using the CERT-RMM Capability Appraisal Method 92

6.4.2 Informal Diagnosis 94

6.5 Planning CERT-RMM-Based Improvements 95

6.5.1 Analyzing Gaps 95

6.5.2 Planning Practice Instantiation 95
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORGANIZATIONAL TRAINING AND AWARENESS</td>
<td>653</td>
</tr>
<tr>
<td>PEOPLE MANAGEMENT</td>
<td>685</td>
</tr>
<tr>
<td>RISK MANAGEMENT</td>
<td>717</td>
</tr>
<tr>
<td>RESILIENCE REQUIREMENTS DEVELOPMENT</td>
<td>747</td>
</tr>
<tr>
<td>RESILIENCE REQUIREMENTS MANAGEMENT</td>
<td>771</td>
</tr>
<tr>
<td>RESILIENT TECHNICAL SOLUTION ENGINEERING</td>
<td>793</td>
</tr>
<tr>
<td>SERVICE CONTINUITY</td>
<td>831</td>
</tr>
<tr>
<td>TECHNOLOGY MANAGEMENT</td>
<td>869</td>
</tr>
<tr>
<td>VULNERABILITY ANALYSIS AND RESOLUTION</td>
<td>915</td>
</tr>
<tr>
<td><strong>PART FOUR—THE APPENDICES</strong></td>
<td>943</td>
</tr>
<tr>
<td>A GENERIC GOALS AND PRACTICES</td>
<td>945</td>
</tr>
<tr>
<td>B TARGETED IMPROVEMENT ROADMAPS</td>
<td>957</td>
</tr>
<tr>
<td>C GLOSSARY OF TERMS</td>
<td>965</td>
</tr>
<tr>
<td>D ACRONYMS AND INITIALISMS</td>
<td>989</td>
</tr>
<tr>
<td>E REFERENCES</td>
<td>993</td>
</tr>
<tr>
<td><strong>BOOK CONTRIBUTORS</strong></td>
<td>997</td>
</tr>
<tr>
<td>INDEX</td>
<td>1001</td>
</tr>
</tbody>
</table>
This page intentionally left blank
We hear the word *resilience* everywhere these days. People are described as resilient when they bounce back from adversity. Things are described as resilient when they can withstand unusual wear and tear and still perform adequately. Organizations are described as resilient when they can meet their mission in the face of adversity and an ever-changing risk environment.

For something or somebody to be described as resilient, a few basic conditions must be met. First, a physical or logical impact must be able to be tolerated for some period of time. Second, the object or person must be able to continue its purpose or mission while impacted. And third, the object or person must be able, in some reasonable time, to return to a “normal” state.

The authors of this book have often struggled with finding the right metaphor for describing resilience. But we always seem to come back to something that everyone understands: a childhood toy called a “Slinky.”

Nearly everyone growing up either had a Slinky or knew someone who did. There wasn’t much to it—a coiled piece of wire that could do some basic tricks—but for the most part, it just kept us amused until we found something else to which to direct our attention. That is, until we tested the limits of the Slinky. Slinkys were mostly forgiving of our attempts to make them do things that weren’t intended by the designers, but there was always that one thing we did that pushed the Slinky

---

to its limits. And the result? The spring became a mere wire, unable to bounce back to its original shape and never again to magically crawl down the stairs on its own.

People, things, and especially organizations can be very much like Slinkys. Most organizations can manage to expand and contract as necessary to absorb the “punch” of disruption. But when the expansion is beyond sustainable limits, in either impact or duration, the organization transforms from a Slinky to a mere wire—unable to spring back to a normal operating condition. Organizations that do not operate with a conscious eye to what their Slinky looks like do so to their own peril. Consider:

- In 2007 the Economist Intelligence Unit surveyed 181 executives from around the world about business resilience. Not surprisingly, 47% of respondents said that they could endure less than one day of downtime from IT systems before the disruption would seriously jeopardize the survival of the entire company [Economist 2007].
- A National Archives and Records Administration survey cites that 25% of companies that experienced an IT outage of two to six days went bankrupt immediately [Economist 2007]. This same study found that 93% of companies that lost their data center for ten days or more filed for bankruptcy within a year.

And it isn’t as though organizations don’t understand the necessity of improving their operational resilience capabilities. In a 2008 Carnegie Mellon CyLab report on Enterprise Security Governance, nearly 50% of survey respondents indicated that risk and crisis oversight is important, but only 37% responded that it was a critical governance issue. Thus, board of directors members recognize the importance of operational resilience but don’t feel it’s important enough to do anything about (or don’t know what to do to address it) [Westby 2008].

In its 2007 report The Resilient Economy: Integrating Competitiveness and Security, the Council on Competitiveness makes a compelling argument that the ability of an organization to actively manage resilience will become a key competitive differentiator in the twenty-first century [van Opstal 2007]. The Council’s conclusions frame a business- and economics-centric argument that supports the theories we posed in 2003 about the transformation of the security discipline into one that supports a larger business-driven purpose. Clearly, today that purpose is to ensure the organization is operationally resilient and able to carry out operational risk management activities in a coordinated way, liberated from traditional silos and organizational structures.

The CERT Resilience Management Model was developed to help organizations do this and, in the end, to help them be better Slinkys.
Introducing the CERT Resilience Management Model

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 its operational resilience management system—the plan, program, processes, procedures, practices, and people that are necessary to manage operational resilience—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 under stressful conditions is vital to meeting organizational goals and objectives.

Purpose

CERT-RMM v1.1 is a capability-focused maturity model for process improvement 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 with 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 process improvement experience in software and systems engineering and acquisition. Foundational concepts from CMMI (Capability Maturity Model Integration) 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 during 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 book provides a detailed explanation of the connections between CERT-RMM and the CMMI models.

**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 an 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 Book**

This book 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 an operational resilience management system can be sustained in complex environments and evolving risk landscapes. The effect of increased levels of capability in managing operational resilience on the mission success of high-value services is discussed. Part Two addresses the use 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. In the last chapter of Part Two, CERT-RMM Perspectives, several invited contributing authors share their thoughts about how CERT-RMM can be applied for different purposes. Another describes how his company evaluated CERT-RMM and found it to be “a comprehensive and flexible framework” for helping to meet business resilience objectives.

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.

The appendices of the book provide a detailed treatment of the model’s Generic Goals and Practices, book references, a list of commonly used acronyms, and a reference glossary.

How to Use This Book

Part One of this book 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 different 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 book. 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 about 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 for 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.
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 v1.1 comprises 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 high-value 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 important, 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.

1.1 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 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 1.1 illustrates these 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 by 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 be done only 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 that 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 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 (BICSORT) 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 1.2.

In Figure 1.2, the upper four capabilities (white text) include processes that provide oversight and top-level management. Governance and audit serve as enablers and accelerators. Risk management informs decisions and choices. Strategy serves 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 higher-level 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).1 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?

---

1. FSTC has since been incorporated into the Financial Services Roundtable (www.fsround.org).
In April 2006, CERT introduced the concept of a process improvement model for operational resilience in the technical report *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* [Caralli 2006]. This technical report defined fundamental resilience and process improvement concepts and detailed candidate focus areas (called “capability areas”) that could be included in an eventual model. This document was the foundation for developing the first instantiation of the model.

In May 2007, as a result of work with FSTC, CERT published an initial framework for managing operational resilience in the technical report *Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes* [Caralli 2007]. In this document, the initial outline for a process improvement model for managing operational resilience was published.

In March 2008, a preview version of a process improvement model for managing operational resilience was released by CERT under the title *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 a technical report published in 2010. The model continues to be available by process area at www.cert.org/resilience.

The publication of this book marks the official release of CERT-RMM v1.1. Version 1.1 includes minor changes to process areas resulting from field use and piloting of the model. In addition, version 1.1 introduces the concept of the *operational resilience management system*, which broadly defines the organization’s collective capability and mechanism for managing operational resilience. More about the operational resilience management system can be found in Section 2.2.

**CERT-RMM**

CERT-RMM draws upon and is influenced by many bodies of knowledge and models. Figure 1.3 illustrates these relationships. (See Tables 1.1 and 1.2 for details about the connections between CERT-RMM and CMMI models.)

At the descriptive level of the model, the process areas in CERT-RMM have been either 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 Resiliency Engineering Framework: Code of Practice Crosswalk, Preview Version, 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 management system. These activities are covered in the CMMI for Services model (CMMI-SVC) [CMMI Product Team 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 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.

1.3 CERT-RMM and CMMI Models

CMMI v1.2 includes three integrated models: CMMI for Development, CMMI for Acquisition, and the newly released CMMI for Services. 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 system 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 1.1 provides a summary of the process area connections between CERT-RMM and the CMMI models. Table 1.2 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>
<thead>
<tr>
<th>CMMI Models Process Areas</th>
<th>Equivalent CERT-RMM Process Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRP—Incident Resolution and Prevention (CMMI-SVC only)</td>
<td>IMC—Incident Management and Control</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>MA—Measurement and Analysis</td>
<td>MA—Measurement and Analysis is carried over intact from CMMI.</td>
</tr>
<tr>
<td></td>
<td>In CERT-RMM, MA is directly connected to MON—Monitoring, which explicitly addresses data collection that can be used for MA activities.</td>
</tr>
<tr>
<td>OPD—Organizational Process Definition</td>
<td>OPD—Organizational Process Definition is carried over from CMMI, but development-life-cycle-related activities and examples are deemphasized or eliminated.</td>
</tr>
<tr>
<td>OPF—Organizational Process Focus</td>
<td>OPF—Organizational Process Focus is carried over intact from CMMI.</td>
</tr>
<tr>
<td>OT—Organizational Training</td>
<td>OTA—Organizational Training and Awareness</td>
</tr>
<tr>
<td></td>
<td>OT is expanded to include awareness activities in OTA.</td>
</tr>
<tr>
<td>REQM—Requirements Management</td>
<td>RRM—Resilience Requirements Management</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>RD—Requirements Development</td>
<td>RRD—Resilience Requirements Development</td>
</tr>
<tr>
<td></td>
<td>Basic elements of RD are included in RRM, but practices differ substantially.</td>
</tr>
<tr>
<td>RSKM—Risk Management</td>
<td>RISK—Risk Management</td>
</tr>
<tr>
<td></td>
<td>Basic elements of RSKM are reflected in RISK, but the focus is on operational risk management activities and the enterprise risk management capabilities of the organization.</td>
</tr>
<tr>
<td>SAM—Supplier Agreement Management</td>
<td>EXD—External Dependencies Management</td>
</tr>
<tr>
<td>SCON—Service Continuity (CMMI-SVC only)</td>
<td>SC—Service Continuity</td>
</tr>
<tr>
<td>TS—Technical Solution</td>
<td>RTSE—Resilient Technical Solution Engineering</td>
</tr>
<tr>
<td></td>
<td>RTSE uses TS as the basis for conveying the consideration of resilience attributes as part of the technical solution.</td>
</tr>
</tbody>
</table>
1.4 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, 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 degree to which 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 applica-
tion of process improvement tools and techniques and provide a foundational plat-
form 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-focused model at its
core, it was perfectly suited for the application of CMMI’s capability dimension. Thus,
the model contained in this book constitutes a maturity model that has a capability
dimension. However, this is not the same as a capability maturity model, since CERT-
RMM does not yet provide an organizational expression of maturity. Describing organ-
izational 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 are that a capability maturity model for op-
erational resilience management founded on CERT-RMM is achievable in the future.
This page intentionally left blank
access controls. See also Access Management (AM), 965
establishing identity community, 452–453
for information assets, 525–526
modification management and, 527–528
overview of, 150–151
for technology assets, 882–883
for trusted access. See Identity Management (IM)
Access Management (AM)
achieve specific goals, 161
assign responsibility for, 165–166
collect improvement information, 173–174
correct inconsistencies, 159–160
declared, 965
enable access, 152–155
establish defined process for, 173
establish process governance, 161–162
FISMA compliance, 957
identify and involve relevant stakeholders, 168–169
insider threats and, 964
introductory notes, 149–151
manage and control access, 151–152
manage changes to access privileges, 155–157
manage work product configurations, 168
monitor and control the process, 169–171
monitoring needs of, 586
objectively evaluate adherence, 172
as Operations process area, 57
periodic review of access privileges, 157–159
plan the process, 163
provide resources for, 163–165
purpose, 149
related process areas, 151
review status with higher-level managers, 172
summary of specific goals and practices, 151
train people for, 167
access privileges assign on basis of identity, 451
correct inconsistencies in, 159–160
declared, 965
deprovisioning identity profiles and, 459–460
granting, 152–155
to human resources documents, 440–441
identify invalid identities, 456–457
identity management linked to, 449
manage and control access with, 151–152
manage changes to access, 155–157
manage changes to employment status, 430–431
manage involuntary termination, 432
overview of, 149–151
periodic review of, 157–159
access requests defined, 966
enabling, 152
acculturation, 966
achieve specific goals, generic goals and practices, 945
acronyms, used in this book, 989–992
acting phase, process improvement, 82–83
action plans for conflict mitigation, 755
implementing process action plans, 636
for organizational processes, 634–635
adaptive maintenance defined, 966
of environmental conditions, 285
adherence, objective evaluation of
Access Management, 172
Asset Definition and Management, 144–145
Communications, 206
Compliance, 238
Controls Management, 267–268
Enterprise Focus, 336–337
Environmental Control, 303
External Dependencies Management, 377–378
Financial Resource Management, 408
generic goals and practices, 953
Human Resource Management, 444
Identity Management, 470–471
Incident Management and Control, 508–509
Knowledge and Information Management, 546
Measurement and Analysis, 574–575
Monitoring, 603
Organizational Process Definition, 626–627
Organizational Process Focus, 651
Organizational Training and Awareness, 682–683
People Management, 713
Resilience Requirements Development, 767
Resilience Requirements Management, 789–790
Resilient Technical Solution Engineering, 826–827
Risk Management, 743–744
Service Continuity, 864–865
adherence, objective evaluation of (contd.) Technology Management, 911–912 Vulnerability Analysis and Resolution, 939
ADM. See Asset Definition and Management (ADM)
maintain, 894–895
manage availability of, 890–891
manage capacity of, 895–897
manage integrity of, 881–882
manage interoperability of, 897–899
manage risks, 878–879
mitigate risks, 880–881
perform change management, 887–888
perform configuration management, 883–887
perform release management, 889–890
protect, 874–875
sustain, 891–894

assign responsibility, generic goals and practices, 948–949

assurance case, 967
Assurance for CMMI PRM (Process Reference Model), 109–110
attack pattern, 967
attack surface, 967
attributes, critical attributes of process elements, 609

audits for configuration management, 887
discovery of vulnerabilities, 921
manage external dependencies, 362
in objective evaluation of adherence, 953
perform resilience oversight, 324–325
for process-compliance, 639
review enterprise focus plan, 337
of technology assets, 883–884

authority, assigning
Access Management, 165–166
Asset Definition and Management, 138–139
Communications, 199–200
Compliance, 231–232
Controls Management, 261–262
Enterprise Focus, 330–331
Environmental Control, 296–297
External Dependency Management, 370–371
Financial Resource Management, 402–403
generic goals and practices, 949
Human Resource Management, 437–438
Identity Management, 464–465
Incident Management and Control, 501–502
Knowledge and Information Management, 539
Measurement and Analysis, 569
Organizational Process Definition, 621
Organizational Process Focus, 645–646
Organizational Training and Awareness, 675
People Management, 706–707
Resilience Requirements
Development, 760–761
Resilience Requirements
Management, 782–783
Resilient Technical Solution Engineering, 819
Risk Management, 738
Service Continuity, 858
Technology Management, 904–905
Vulnerability Analysis and Resolution, 933
availability attributes of information assets, 514
defined, 967
Knowledge and Information Management and, 513
of measurement information, 564
availability, of information assets
document organizational and intellectual knowledge of staff, 532–533
duplication and retention, 531–532
overview of, 530–531
availability, of staff
establish redundancy for vital staff, 694–695
manage, 693–694
perform succession planning, 695–697
plan for return-to-work following disruptive events, 700–701
plan to support staff during disruptive events, 698–700
prepare for redeployment, 697–698
availability, of technology assets
maintain technology assets, 894–895
manage technology capacity, 895–897
manage technology interoperability, 897–899
overview of, 890–891
sustain technology assets, 891–894
awareness activity, 967
awareness materials, 659–660
awareness plan, 657–658
awareness program. See also Organizational Training and Awareness (OTA)
assess effectiveness of, 662–663
defined, 967
establish delivery capability, 658–660
establish needs, 655–657
establish plan, 657–658
overview of, 655
perform activities, 660–661

B
back up, of information assets, 531–532
base measures
data collection and, 561–562
defined, 967
specify, 556
baseline competencies
comparing skills inventory to, 416
establishment of, 414–415
baseline verification criteria, acquisition of staff, 419
baselines
baseline configuration item, 968
for change management, 887–888
for configuration management, 887
identifying and assessing risks, 522
resilience requirements, 776
for technology assets, 884
BES (Bulk Electric System), 101–102
BIC-SORT (Best in Class Security and Operations Roundtable), 10–11
BRM (business resilience management), 110–115
budgeting
benefits of CERT-RMM, 6
commit funds for operational resilience management, 383–384
establish financial commitment, 382–383
establish resilience budgets, 388–389
establish structure to support financial management, 384–386
fund resilience activities, 390–391
perform cost and performance analysis, 393–394
resolve funding gaps, 388–389
bugs, availability of technology assets and, 891
builds, release management and, 889–890
Bulk Electric System (BES), 101–102
business case
for adoption of CERT-RMM processes, 81
commit funds for operational resilience management, 383–384
for convergence of operational risk activities, 24–25
fund operational resilience management, 318–319
business continuity plans. See also service continuity plans, 839
business impact analysis, availability of technology assets and, 892
business processes
concept of, 29–30
defined, 968
fueled by assets, 30–33
relationships among services, assets and, 27–28
business requirements. See also resilience requirements, 968
business resilience, downtime tolerance and, xvi
business resilience management (BRM), 110–115
CERT Resiliency Engineering Framework, v0.95R (REF Team 2008b), 12
certification training, Communications, 201
CERT-RMM (CERT Resilience Management Model)
audience for, xviii
benefits to organizations, 3–6
CMMI models and, 15–18
CERT-RMM vs., 18–19
evolution of, 9–12
influences on, 12–15
introduction to, xvii
need for, 3–4
official release of v1.1, 12
overview of, 7–8
process improvement and CMMI models influencing, 8–9
as process improvement model, 2–3
purpose of, xvii–xviii
CERT-RMM concepts
adapting terminology and, 39
disruption and stress, 21–23
elements of operational resilience management, 27–39
operational resilience management, 25–27
CERT-RMM uses for business resilience, 110–115
diagnosing with, 92–95
equivalent CERT-RMM process areas, 15–18
focus of process improvement in, 15
influencing CERT-RMM, 13
for utility sector, 99–104
for work product configurations, 950
Crosswalk, Preview Version, v0.95R (REF Team 2008b), 13
codes of practice
coding guidelines, for resilient software and systems, 803
collect improvement information. See improvement information, collecting
co-location, 968
commitment
establish financial commitment, 382–383
of funds to operational resilience management, 383–384
to incident management plan, 477
to resilience requirements, 774–775
to service continuity plans, 834–835
capacity of technology assets, 895–897
capacity planning, 896, 968
process areas by, 319
process components, 42–44
of risk, 351, 719–720, 727
CERT Resiliency Engineering Framework: Code of Practices
plan the process, 197–198
prepare for, 177
prepare for management of, 183
provide resources for, 198–199
purpose of, 175
related process areas, 176
relationships driving threat/incident management, 58
review status with higher-level managers, 206
summary of specific goals and practices, 176
train people for, 200–201
communications stakeholders, 968
collection and preservation of evidence and, 482
converting compliance activities into improvement activities, 6
defined, 968
developing program for, 212–214
evaluating adherence to. See adherence, objective evaluation of performing resilience oversight, 324
Compliance (COMP)
achieve specific goals, 227
analyze obligations for, 217–218
assign responsibility for, 231–232
collect and validate compliance data, 219–225
collect improvement information, 239–240
defined, 968
demonstrate extent of satisfaction of obligations, 221–223
evaluate defined process, 239
establish guidelines and standards, 214
establish obligations for, 215–217
establish ownership for meeting obligations, 218–219
establish plan for, 211–212
establish process governance, 227–228
establish program for, 212–214
identify and involve relevant stakeholders, 234–236
introduction notes, 209–210
manage work product configurations, 234
monitor activities of, 225–226
monitor and control the process, 236–237
objectively evaluate adherence, 238
plan the process, 229
prepare for compliance management, 210–211
provide resources for, 229–231
purpose of, 209
related process areas, 210
remediate areas of non-compliance, 223–225
review status with higher-level managers, 238
summary of specific goals and practices, 210
train people for, 232–233
collaboration knowledgebase, 969
collaboration obligations, 969
collaboration office, defining and installing, 212
collaboration components, model defined, 981
evaluated components, 43–44, 48, 972
informational component, 43–44, 48, 975
numbering scheme, 47–49
process area component categories, 42–44
process area components, descriptions, 44–47
process areas and their categories, 41–42
required components, 43–44, 48, 981
typographical and structural conventions, 49–51
computer security incident response team (CSIRT), 476
collaboration definitions, 969
confidentiality
access controls and, 525–526
agreements, 429–430
attributes of information assets, 514
defined, 969
disposal management, 526–527
encrypt high-value information, 524–525
Knowledge and Information Management process area
and, 513
of measurement information, 564
overview of, 523–524
configuration items, 969
configuration management
defined, 969
for information assets, 529
for technology assets, 883–887
work product configurations and, 950
conflict resolution
identify and resolve conflicts in service continuity plans, 846
mitigation action plans, 755
consistency vs. flexibility, 611
constellation, 969
containers
defined, 969
managing information asset risk in, 321
contingency plans. See service continuity plans
continuity of operations. See also Service Continuity (SC), 969
continuous representation, of CERT-RMM structure, 68–69
contracts, with external entities, 360–362
control objectives
analysis of controls to ensure, 250–252
assessment process for, 253–257
defining, 244–246
establishing controls to meet, 246–248
identifying and establishing controls, 248–250
overview of, 244
controls. See also monitor and control access. See administrative (management) controls
defined, 969–970
external dependencies management, 361
for incident management, 506–508
for information assets, 519–521
internal, 975
manage work product configurations and, 950
revision plan, 732
for risk mitigation, 732
for technology assets, 875–878
for validity and reliability of information assets, 529–530
Controls Management (CTRL)
achieve specific goals, 257
analyze controls, 250–253
assess control effectiveness, 253–257
assign responsibility for, 261–262
collect improvement information, 269–270
define controls, 248–250
defined, 970
as Engineering process area, 56
establish control objectives, 244–246
establish controls supporting objectives, 246–248
establish defined process for, 269
establish process governance, 257–259
FISMA compliance, 959
identify and involve relevant stakeholders, 264–265
insider threats and, 964
introductory notes, 241–243
manage work product configurations, 264
managing changes to protecting and sustaining services and assets, 131
managing overall internal control system in, 151
monitor and control process, 265–267
objectively evaluate adherence, 267–268
plan process, 259
provide resources, 259–261
purpose of, 241
related process areas, 243
relationships driving threat/incident management, 58
review status with higher-level managers, 268
summary of specific goals and practices, 244
train people for, 262–263
convergence defined, 970
of operational risk management activities, 23–25
convergence advantage of CERT-RMM, 5–6
defined, 7
coordination communications, 187
corrective measures for access privileges, 159–160
for controls management, 247
defined, 970
for enterprise focus, 325–326, 336–337
for environmental conditions, 285
for inconsistencies in identity community, 457–459
monitoring and controlling and, 952–953
for performance issues, 325–326
cost of resilience, 970
costs. See also Financial Resource Management (FRM)
external dependencies management, 362
of non-compliance, 222–223
used to track and document resilience management, 392–393
credentialing, 970
crisis
defined, 970
governance, xvi
critical success factors, 970
cross-training, 970
The Crosswalk, 13
cryptography. See encryption
CSIRT (computer security incident response team), 476
CTRL. See Controls Management (CTRL)
cultural norms, stress of managing globalization risks, 23
curriculum, for managing global information assets, 668
custodians
of access management, 159–160, 168–169
of asset definition and management, 126–130
defining, 33
of environmental control, 296–297
custodians, asset conformity to resilience requirements, 778
defined, 966
resilience requirements and, 774–775
damage control, responding to incidents, 489
dashboard, governance, 324
data analysis. See also Measurement and Analysis (MA)
of measurement data, 562–563
methods and tools, 559–560
data collection
collection standards and guidelines, 589–591
of compliance data, 219–221
of measurement data, 561–562
monitoring and, 577–579, 588–589
of monitoring data, 591–592
techniques for, 557–559
vulnerability data collection, 921–922
Data Collection and Logging, Process Management, 58–59
data storage, 563–564
databases
for change management, 888
for configuration management, 886
identify external dependencies, 344–347
identify vital organizational, 837–839
incident knowledgebase, 922
of service continuity plans, 843
Davis, Noopur, 115
defined process
Access Management, 173
Asset Definition and Management, 145–146
<table>
<thead>
<tr>
<th>Index 1007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications, 207</td>
</tr>
<tr>
<td>Compliance, 239</td>
</tr>
<tr>
<td>Controls Management, 269</td>
</tr>
<tr>
<td>defined, 970</td>
</tr>
<tr>
<td>Enterprise Focus, 337–338</td>
</tr>
<tr>
<td>Environmental Control, 304</td>
</tr>
<tr>
<td>External Dependencies</td>
</tr>
<tr>
<td>Financial Resource Management, 409</td>
</tr>
<tr>
<td>generic goals and practices, 934</td>
</tr>
<tr>
<td>Human Resource Management, 445</td>
</tr>
<tr>
<td>Identity Management, 471</td>
</tr>
<tr>
<td>Incident Management and Control, 510</td>
</tr>
<tr>
<td>Knowledge and Information Management, 547–548</td>
</tr>
<tr>
<td>Measurement and Analysis, 575–576</td>
</tr>
<tr>
<td>Monitoring, 604</td>
</tr>
<tr>
<td>Organizational Process Definition, 627–628</td>
</tr>
<tr>
<td>Organizational Process Focus, 632</td>
</tr>
<tr>
<td>Organizational Training and Awareness, 683</td>
</tr>
<tr>
<td>overview of, 72</td>
</tr>
<tr>
<td>People Management, 714</td>
</tr>
<tr>
<td>Resilience Requirements Development, 768–769</td>
</tr>
<tr>
<td>Resilience Requirements Management, 791</td>
</tr>
<tr>
<td>Resilient Technical Solution Engineering, 827–828</td>
</tr>
<tr>
<td>Risk Management, 744–745</td>
</tr>
<tr>
<td>Service Continuity, 865–866</td>
</tr>
<tr>
<td>Technology Management, 912–913</td>
</tr>
<tr>
<td>Vulnerability Analysis and Resolution, 940</td>
</tr>
<tr>
<td>deliver communications</td>
</tr>
<tr>
<td>identify methods and channels, 188–190</td>
</tr>
<tr>
<td>overview of, 188</td>
</tr>
<tr>
<td>delivery capability</td>
</tr>
<tr>
<td>for training program, 666–668</td>
</tr>
<tr>
<td>Deming, Edward, 80, 82</td>
</tr>
<tr>
<td>dependencies</td>
</tr>
<tr>
<td>identify, 837</td>
</tr>
<tr>
<td>manage external. See External Dependencies Management (EXD)</td>
</tr>
<tr>
<td>manage on public infrastructure for facilities, 288–289</td>
</tr>
<tr>
<td>manage on public services for facilities, 287</td>
</tr>
<tr>
<td>deploy practices, using CERT-RMM as organizing structure for, 79–80</td>
</tr>
<tr>
<td>deploy process assets</td>
</tr>
<tr>
<td>monitoring implementation, 639</td>
</tr>
<tr>
<td>overview of, 636–637</td>
</tr>
<tr>
<td>standard processes, 638</td>
</tr>
<tr>
<td>deprovisioning identities</td>
</tr>
<tr>
<td>correcting inconsistencies in identity community, 458–459</td>
</tr>
<tr>
<td>defined, 970</td>
</tr>
<tr>
<td>introduction to, 448–449</td>
</tr>
<tr>
<td>involving stakeholders in, 468</td>
</tr>
<tr>
<td>overview of, 459–460</td>
</tr>
<tr>
<td>derived measures</td>
</tr>
<tr>
<td>data sets for, 563</td>
</tr>
<tr>
<td>defined, 971</td>
</tr>
<tr>
<td>specifying, 556</td>
</tr>
<tr>
<td>descriptive statistics, in data analysis, 560</td>
</tr>
<tr>
<td>design guidelines, for resilient software and systems, 801–802</td>
</tr>
<tr>
<td>detective controls, 247–248</td>
</tr>
<tr>
<td>development lifecycle, software and systems, 793</td>
</tr>
<tr>
<td>development plans, for resilient technical solutions creating, 807–808</td>
</tr>
<tr>
<td>integrating selected guidelines with, 809–810</td>
</tr>
<tr>
<td>monitor execution of, 810–812</td>
</tr>
<tr>
<td>release solutions into production, 812–813</td>
</tr>
<tr>
<td>select and tailor guidelines for, 808–809</td>
</tr>
<tr>
<td>diagnosing phase, process improvement defined, 82–83</td>
</tr>
<tr>
<td>formal diagnosis using Capability Appraisal Method, 92–94</td>
</tr>
<tr>
<td>informal diagnosis, 94–95</td>
</tr>
<tr>
<td>planning CERT-RMM-based improvements, 95–97</td>
</tr>
<tr>
<td>diagnosis of current resilience practices formal, using Capability Appraisal Method, 92–94</td>
</tr>
<tr>
<td>informal, 94–95</td>
</tr>
<tr>
<td>digital information, stress of managing intangible assets, 22</td>
</tr>
<tr>
<td>disciplinary action, for violation of resilience policies, 426–427</td>
</tr>
<tr>
<td>disposition (disposal) defined, 971</td>
</tr>
<tr>
<td>of information assets, 526–527</td>
</tr>
<tr>
<td>dispute resolution, external dependencies management, 362 disruptive events</td>
</tr>
<tr>
<td>identifying staff risks, 691</td>
</tr>
<tr>
<td>managing staff availability during, 693</td>
</tr>
<tr>
<td>plan for return-to-work following, 700–701</td>
</tr>
<tr>
<td>plan to support staff during, 698–700</td>
</tr>
<tr>
<td>prepare for redeployment of staff during, 697–698</td>
</tr>
<tr>
<td>distribution, of monitoring information, 592–594</td>
</tr>
<tr>
<td>DNA, identity's defined, 450</td>
</tr>
<tr>
<td>understanding, 447–448</td>
</tr>
<tr>
<td>documentation</td>
</tr>
<tr>
<td>in asset definition and management, 146–147</td>
</tr>
<tr>
<td>of awareness needs, 657</td>
</tr>
<tr>
<td>of changes to process assets, 637</td>
</tr>
<tr>
<td>of changes to resilience requirements, 776</td>
</tr>
<tr>
<td>of commitments to resilience requirements, 774–775</td>
</tr>
<tr>
<td>of commitments to service continuity plans, 834</td>
</tr>
<tr>
<td>of communications, 194, 197, 207–208</td>
</tr>
<tr>
<td>of compliance, 223, 239–240</td>
</tr>
<tr>
<td>of controls management, 245–246, 269–270</td>
</tr>
<tr>
<td>of disciplinary action, 426–427</td>
</tr>
<tr>
<td>of environmental controls, 277, 286–290, 305</td>
</tr>
<tr>
<td>event detection and, 479</td>
</tr>
<tr>
<td>of external dependencies management, 361</td>
</tr>
<tr>
<td>in financial resource management, 388, 392–394, 400</td>
</tr>
<tr>
<td>in human resource management, 419, 422, 435–436</td>
</tr>
<tr>
<td>of improvement information, 955</td>
</tr>
<tr>
<td>of incident analysis, 486</td>
</tr>
<tr>
<td>of incident evidence, 481–482</td>
</tr>
<tr>
<td>incident management plan and, 476</td>
</tr>
<tr>
<td>of inconsistencies in resilience requirements, 778</td>
</tr>
<tr>
<td>of maintenance operations, 895</td>
</tr>
<tr>
<td>of measurement objectives, 555</td>
</tr>
<tr>
<td>post-incident review and, 494</td>
</tr>
<tr>
<td>of return-to-work plan, 700</td>
</tr>
<tr>
<td>of risk measurement criteria, 723</td>
</tr>
<tr>
<td>of scope of vulnerabilities, 917</td>
</tr>
<tr>
<td>of service continuity plans, 840–842</td>
</tr>
</tbody>
</table>
as Engineering process area, 56
establish corrective actions, 325–326
establish critical success factors, 310–312
establish defined process, 337–338
establish organizational services, 312–314
establish process governance, 327–328
establish resilience as governance focus area, 322–323
establish sponsorship, 317
establish strategic objectives, 309–310
FISMA compliance, 958
identify and involve relevant stakeholders, 332–333
identify communications requirements with, 180
introductions to, 307–308
manage work product configurations, 332
monitor and control the process, 333–336
objectively evaluate adherence, 336–337
perform resilience oversight, 324–325
plan for operational resilience, 314–317
plan the process, 328–330
promoting resilience-aware culture, 319–320
provide resilience oversight, 321–322
provide resources for, 328–329
purpose of, 307
related process areas, 308
relationships driving threat/incident management, 58
review status with higher-level managers, 337
summary of specific goals and practices, 308
train people for, 331
enterprise level monitoring, 579
policies, 971
specifications for external entities, 333–354
enterprise management, aspects of CERT-RMM, 14–15
Enterprise Management process areas
COMM. See Communications (COMM)
COMP. See Compliance (COMP) defined, 7–8
EF. See Enterprise Focus (EF)
FRM. See Financial Resource Management (FRM)
HRM. See Human Resource Management (HRM) model view of, 54–55
OTA. See Organizational Training and Awareness (OTA) overview of, 41–43
RISK. See Risk Management (RISK) enterprise-level controls as administrative controls, 246
assessing effectiveness of, 253–254
creating, 248–250
defined, 242
enterprise-level resilience requirements assigning to services, 753–754
defined, 971
establishing, 751–752
identifying, 750
overview of, 748
entities, creating identities for. See Identity Management (IM)
Environmental Control (EC) achieve specific goals, 290
assign resilience requirements to facility assets, 276–277
assign responsibility for, 296–297
Cloud Computing and, 963
collect improvement information, 304–305
control operational environments, 282–283
defined, 971
establish and implement controls, 277–280
establish defined process, 304
establish process governance, 290–292
establish resilience-focused facility assets, 275
FISMA compliance, 958
identify and involve relevant stakeholders, 299–300
introductory notes, 271–272
maintain environmental conditions, 285–286
manage dependencies on public infrastructure, 288–289
manage dependencies on public services, 287
manage facility asset risk, 280–282
manage work product configurations, 298–299
monitor and control the process, 300–302
monitor needs of, 386
objectively evaluate adherence, 303
as Operations process area, 57
perform facility sustainability planning, 284–285
plan for facility retirement, 289–290
plan the process, 292–293
prioritize facility assets, 273–274

E
EC. See Environmental Control (EC)
EF. See Enterprise Focus (EF)
emergency actions, responding to incidents, 489
employment. See Human Resource Management (HRM)
employment agreements, 420–422
employment status, managing changes to manage access to assets, 430–431
manage impact of position changes, 428–430
manage involuntary terminations, 431–432
overview of, 427–428
encryption
cryptographic controls, 970
of high-value information, 524–525
policies, 971
Engineering process areas
ADM. See Asset Definition and Management (ADM)
CTRL. See Controls Management (CTRL) defined, 7–8
model view of, 56
overview of, 41–43
RRD. See Resilience Requirements Development (RRD)
RRM. See Resilience Requirements Management (RRM)
RTSE. See Resilient Technical Solution Engineering (RTSE)
SC. See Service Continuity (SC)
Enterprise Focus (EF) achieve specific goals, 325–326
assign responsibility for, 330–331
collect improvement information, 338–339
commit funding for operational resilience management, 318–319
defined, 971
of service continuity tests, 848
of succession plan, 696
of support for staff during disruptive events, 699
of training needs, 665
of vulnerability analysis and resolution strategy, 919
downtime
business resilience and, xvi
planned, 890, 979
unplanned, 890, 987
due diligence, performing on candidate external entities, 359
duplication, of information assets, 531–532
establish process governance.

events
event triage
event logging, in incident
evaluation
event detection
analyzing and triaging events,
collecting, documenting, and
preserving event evidence,
establishing process for,
logging and tracking events,
monitoring, identifying, and
reporting events,
transitioning from detection to
declaration,
event logging, in incident
management,
event triage
defined, overview of,
events
defined, disruptive

evidence collection, responding to incidents,
example blocks, process area
defined, typographical and structural
conventions, 51

EXD. See External Dependencies Management (EXD)
exercises. See also test (exercise)
service continuity plans, exit interview process,
expected components
defined, overview of, summary of,
expenditures, optimizing resilience
determine return on investments,
identify cost recovery opportunities,
overview of,
expense requests, funding resilience activities,
experience, incorporating into process
establish resilience-focused,
external dependencies, External Dependencies Management (EXD)
achieve specific goals, assign responsibility for,
Cloud Computing and,
collect improvement information,
defined, develop resilient software across life cycle with,
establish defined process,
establish enterprise specifications for,
establish formal relationships,
establish process governance,
establish resilience specifications for,
establish resilience specifications for,
evolve and select external entities,
formalize relationships,
identify and involve relevant stakeholders,
recognize external dependencies,
recognize risks associated with external dependencies,
introductory notes,
Ascertaining expertise and performance,
managing work product configurations,
managing dependencies on public infrastructure for,
monitor and control services for,
plan for retirement of,
plan process for,
prioritization of,
protect, provide resources for,
review status with higher-level managers,
risk mitigation strategies for,
train people for,
train people, 371–372

F
facilities. See also Asset Definition and Management (ADM) and Environmental Control (EC)
facility assets. See also Asset Definition and Management (ADM)
access privileges focusing on,
achieve specific goals, assign resilience requirements to,
assign responsibility for,
in CERT-RMM, collect improvement information,
controlling operational environment,
defined, establish and implement controls for,
establish process governance for,
establish resilience-focused,
identify and assess risk for,
identify and involve relevant stakeholders,
lifecycle of,
manage work product configurations,
managing dependencies on public infrastructure for,
monitor and control services for,
perform sustainability planning,
plan for retirement of,
plan process for,
prioritization of,
protect, provide resources for,
review status with higher-level managers,
risk mitigation strategies for,
train people, 297–298
Federal Energy Regulatory Commission (FERC), 101–102

correcting inconsistencies in identity community, 458
defined, 447, 972
of identities, 468

FERC (Federal Energy Regulatory Commission), 101–102

federations

financial commitment, establishing
establish structure to support, 384–386
for operational resilience management, 383–384
overview of, 382–383
financial exceptions, in cost and performance analysis, 394

Financial Resource Management (FRM)
account for resilience activities, 392–394
achieve specific goals, 398
assign responsibility for, 402–403
collect improvement information, 410
commit funding for operational resilience management, 383–384
defined, 972
Enterprise Management and, 54–55
establish defined process, 409
establish financial commitment, 382–383
establish process governance, 398–400
establish structure to support financial management, 384–386
fund resilience activities, 390–391
identify and involve relevant stakeholders, 404–406
introductory notes, 381–382
manage work product configurations, 404
monitor and control the process, 406–407
objectively evaluate adherence, 408
optimize resilience expenditures and investments, 394–398
perform financial planning, 386–390
plan the process, 400
provide resources for, 400–402
purpose of, 391
related process areas, 382
review status with higher-level managers, 409
summary of specific goals and practices, 382
train people for, 403–404

Financial Services Technology Consortium (FTSC), 11

fuzz testing, 972

G
general guidelines, for Resilient Technical Solution Engineering, 798–800
generic goals and practices
applying, 74
assign responsibility, 948–949
capability levels related to, 69–73
collect improvement information, 955
defined, 46–48, 972–973
elaborations, 74
establish defined process, 954
establish process governance, 946
identify and involve relevant stakeholders, 951
manage work product configurations, 950
monitor and control the process, 951–953
objectively evaluate adherence, 953
perform specific practices, 943
plan the process, 946–947
process areas supporting, 74–75
provide resources, 948
review status with higher-level managers, 953
tags and numbering scheme for, 49
train people, 949–950
typographical and structural conventions, 50
understanding, 73
using practice-level scope, 88–89
geographical controls
establishing and managing. See Environmental Control (EC)
for operational environment, 283
geographical dispersion, 973
geopolitical shifts, stress of managing globalization risks, 23
global economy, stress of managing operational risk in, 22–23
globalization, operational resilience management and, 2
goals. See also objectives
establishing resilience through goals and objectives, 423–424
generic. See generic goals and practices
measure performance against goals and objectives, 425–426
governance, process
Access Management, 161–162
Asset Definition and Management, 133–136
Communications, 196–197
Compliance, 212, 227–228
Controls Management, 241, 257–259
defined, 973
Enterprise Focus, 327–328
Environmental Control, 290–292
establish corrective actions, 325–326
establish resilience as focus area of, 322–323
External Dependencies
Management, 366–367
Financial Resource Management, 398–400
generic goals and practices, 946
Human Resource Management, 433–435
Identity Management, 460–462
Incident Management and Control, 497–498
Knowledge and Information Management, 534–536
Measurement and Analysis, 566–567
Monitoring, 594–595
Organizational Process Definition, 617–618
Organizational Process Focus, 641–643
Organizational Training and Awareness, 671–673
People Management (PM), 701–703
perform resilience oversight, 323–325
provide resilience oversight, 321–322
Resilience Requirements
Development, 757–758
Resilience Requirements Management, 779–780
Resilient Technical Solution Engineering, 814–815
risk and crisis oversight and, xvi
Risk Management, 734–735
Service Continuity, 853–855
Technology Management, 899–901
Vulnerability Analysis and Resolution, 929–930
grid modernization, electric power industry, 103–104
guidance, using CERT-RMM as basis for, 78–79
guidelines. See also standards for configuration management, 886
establish tailoring criteria and, 610–612
for handling information assets, 517
for integrated teams, 615–616
for monitoring, 589–591
for resilience, 320–321
for service continuity, 833
guidelines, for resilient technical solutions
identify architecture and design guidelines, 801–802
identify assembly and integration guidelines, 805–807
identify general guidelines, 798–800
identify implementation guidelines, 802–805
identify requirements guidelines, 800–801
integrating selected guidelines with software and system development process, 809–810
select and tailor, 808–809

H
hardware, integrity of, 882
hazards, service continuity planning and, 832
higher-level managers, reviewing with Access Management, 172
Asset Definition and Management, 145
Communications, 206
Compliance, 238
Controls Management, 268–269
Enterprise Focus, 337
Environmental Control, 304
External Dependencies Management, 378
Financial Resource Management, 409
generic goals and practices, 953
Human Resource Management, 445
Identity Management, 471
Incident Management and Control, 509
Knowledge and Information Management, 547
Measurement and Analysis, 575
Monitoring, 603
Organizational Process Definition, 627
Organizational Process Focus, 651
Organizational Training and Awareness, 683
People Management (PM), 714
Resilience Requirements Development, 768
Resilience Requirements Management, 790–791
Resilient Technical Solution Engineering, 827
Risk Management, 744
Service Continuity, 865
Technology Management, 912
Vulnerability Analysis and Resolution, 940
Highfill, Darren, 99–100
high-value assets
defined, 973
metrics for, 893
high-value information, encryption of, 524–525
high-value services
defined, 973
as focus of CERT-RMM, 29
identify and prioritize, 835–836
identify internal and external dependencies and interdependencies, 837
identify vital organizational records and databases, 837–839
prioritization of technology assets related to, 871–872
resilience requirements for, 33–35
Human Resource Management (HRM) achieve specific goals, 433
address skill deficiencies, 416–418
assign responsibility for, 437–438
collect improvement information, 445–446
defined, 973
Enterprise Management and, 54–55
establish baseline competencies, 414–415
establish defined process, 445
establish disciplinary process, 426–427
establish process governance, 433–435
establish resilience as job responsibility, 423
establish resilience performance goals/objectives, 423–425
establish resource needs, 413
identify and involve relevant stakeholders, 441–442
insider threats and, 963–964
introductory notes, 411–412
inventory skills and identify gaps, 415–416
manage changes to employment status, 412, 427–432
manage staff acquisition, 418–422
manage staff performance. See performance, in staff management
manage work product configurations, 440–441
measure and assess performance, 425–426
Human Resource Management (HRM)
(contd.)
monitor and control the process, 442–444
objectively evaluate adherence, 444
plan the process, 435–436
provide resources for, 436–437
purpose of, 411
related process areas, 412
review status with higher-level managers, 445
summary of specific goals and practices, 413
train people for, 439–440

icons, process area, 42–43
IDEAL model, 82–83
identify and involve relevant stakeholders. See stakeholders, identify and involve identities
assign roles to, 453–454
correct inconsistencies in, 457–459
creating, 450–451
defined, 973
deprovision, 459–460
defining identity community, 452–453
manage, 454
monitor and manage changes to, 455–456
overview of, 449–450
periodically review/maintain, 456–457
identity community
assigning roles to identities, 453–454
correcting inconsistencies in, 457–459
defining, 973
establishing, 452–453
monitoring and managing changes in, 455–456
periodic review of, 456–457
Identity Management (IM).
See also Access Management (AM); Risk Management (RISK)
achieve specific goals, 460
assign responsibility for, 464–465
assign roles to identities, 453–454
collect improvement information, 471–472
create identities, 450–451
defining, 973
enable access request and approval, 152
establish defined process, 471
establish identities, 449–450
establish identity community, 452–453
establish process governance, 460–462
FISMA compliance, 958
identify and involve relevant stakeholders, 467–468
introductory notes, 447–449
manage work product configurations, 466–467
monitor and control the process, 468–470
monitoring needs of, 586
objectively evaluate adherence, 470–471
as Operations process area, 57
plan the process, 462
provide resources for, 462–464
purpose of, 447
related process areas, 449
review status with higher-level managers, 471
specific goals and practices, 449
train people for, 465–466
identity profiles, 973
identity registration, 974
identity repository, 974
IM. See Identity Management (IM)
IMC. See Incident Management and Control (IMC)
impact valuation, 974
implementation guidelines, for resilient software and systems, 802–803
improvement information, collecting Access Management, 173–174
Asset Definition and Management, 146–147
Communications, 207–208
Compliance, 239–240
Controls Management, 269–270
Enterprise Focus, 338–339
Environmental Control, 304–305
External Dependencies
Management, 379–380
Financial Resource Management, 410
generic goals and practices, 955
Human Resource Management, 445–446
Identity Management, 471–472
Incident Management and Control, 510–511
Knowledge and Information Management, 548–549
Measurement and Analysis, 576
Monitoring, 604–605
Organizational Process Definition, 628
Organizational Process Focus, 652
Organizational Training and Awareness, 684
People Management, 714–715
for process areas, 202
Resilience Requirements Development, 769
Resilience Requirements Management, 791–792
Resilient Technical Solution Engineering, 828–829
Risk Management, 745–746
Service Continuity, 866–867
Technology Management, 913–914
Vulnerability Analysis and Resolution, 940–941
improvement mind-set, benefits of CERT-RMM, 6
inappropriate behavior, identifying staff risks, 691
incident closure, 492–493, 974
incident declaration
analyzing incidents, 483–486
criteria for, 484–485
to support response, 483–484
incident escalation
communications and, 187
defined, 974
Incident Management and Control, 487–488
incident life cycle, 974
Incident Management and Control (IMC)
achieve specific goals, 497
analyze and triage events, 482–483
analyze incidents, 485–486
assign responsibility for, 501–502
assign staff for, 477–478
close incidents, 492–493
collect, document, and preserve event evidence, 481–482
collect improvement information, 510–511
communicate incidents, 490–492
declare events for response planning, 483–484
define criteria for event declaration, 484–485
defining, 974
detect and report events, 478–479
escalate incidents, 487–488
establish defined process, 510
establish process for, 475–476
establish process governance, 497–498
FISMA compliance, 959
identify and involve relevant stakeholders, 504–506
identify communications requirements, 180
integrate incident handling with problem management, 494–495
introductory notes, 473–475
learn from incidents, 493
log and track events, 480–481
manage work product configurations, 504
monitor and control the process, 506–508
monitoring needs of, 586
objectively evaluate adherence, 508–509
plan for, 476–477
plan the process, 498–499
post-incident review, 493–494
provide resources for, 499–500
purpose of, 473
related process areas, 475
relationships driving threat/incident management, 57–58
respond to/ recover from incidents, 487–490
review status with higher-level managers, 509
summary of specific goals and practices, 475
train people, 502–503
translate lessons into strategy, 495–496
incident owner, 974
incident response
closing incidents, 492–493
communication in, 490–492
defined, 974
developing and implementing, 488–490
escalation of incidents, 487–488
establishing process for, 487
incident stakeholder, 974
incidents, 974
incomplete process, capability level 0, 70
informal diagnosis, of current resilience practices, 94–95
information. See also Asset Definition and Management (ADM) and Knowledge and Information Management (KIM)
access privileges focusing on, 153
as asset in CERT-RMM, 31–32
establishing compliance
knowledgebase or repository, 220–221
identifying external dependencies, 344–347
life-cycle of, 37
objective views for, 59, 61
processing cycle, 529–530
protecting and sustaining, 35–36
resilience requirements for, 33–35
information asset baseline, 974
information asset categorization, 975
information asset container, 975
information asset owner, 975
information assets
defining. See Asset Definition and Management (ADM)
definition of, 974
managing. See Knowledge and Information Management (KIM)
information technology. See IT (information technology)
informative component
defined, 975
overview of, 43–44
summary of, 48
infrastructure
for communications, 190–191
managing dependencies on public, 288–289
for monitoring, 588–589
initialisms, acronyms used in this book, 989–992
initiating phase, process improvement.
See also objectives, setting and communicating, 82
insider threats, 963
inspections, product release and, 812–813
institutional knowledge. See organizational and intellectual knowledge
institutionalization
capability levels and, 68–69
CERT-RMM as organizing structure for, 80
CERT-RMM generic goals and practices, 73–74
connecting capability levels to, 69–73
defined, 975
defined process. See defined process managed process
overview of, 67
process areas supporting generic practices, 74–75
instructors
for awareness program, 659–660
for training program, 667
intangible assets, stress of managing, 22
integrated teams, establish rules and guidelines for, 615–616
integration guidelines, for Resilient Technical Solution Engineering, 803–807
integrity
checks, 221, 562
data analysis and, 561–562
defined, 975
Knowledge and Information Management and, 513
of measurement information, 564
integrity, of technology assets
access controls, 882–883
overview of, 881–882
perform change management, 887–888
perform configuration management, 883–887
perform release management, 889–890
integrity of information assets
attributes, 514
configuration management, 529
modification management, 527–528
overview of, 527
validity and reliability, 529–530
intellectual property
contrasted with institutional knowledge, 532
defined, 975
protecting, 513
interdependencies, identify internal and external dependencies, 837
internal communications. See also Communications (COMM), 186–187
internal control system
assessing effectiveness of, 253–254
defined, 975
implementing for facility assets, 277–280
overview of, 241–242
interoperability
defined, 986
of technology assets, 897–899
interviews, to assess effectiveness of awareness program, 662
Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes (Caralli 2007), 12
inventory. See also repositories of assets, 124–125
of compliance obligations, 216–217
maintaining changes to assets and, 133–134
of service continuity plans, 843
of skills, 415–416, 985
of staff, 688
of stored data, 564
investigation reports, in establishing disciplinary process, 427
investments, resilience
determining return on, 396–397
investments, resilience (contd.)
identify cost recovery opportunities, 397–398
optimize resilience expenditures and, 394–396
involuntary termination of employment managing, 431–432
overview of, 428
IT (information technology)
evolution of CERT-RMM, 9–12
managing operational risk for, 23
as traditional focus of operational risk management, 8–9

J
job descriptions
creating to reflect base competencies, 415
developing requisitions for unfilled positions, 417–418
establishing terms and conditions of employment, 420–422
incident management plan and, 477
inserting resilience obligations in, 423
updating to incorporate missing skills, 417
job-specific verification criteria, 419–420

K
key control indicators (KCIs)
defined, 975
performing resilience oversight, 325
key indicators
establish corrective actions, 325–326
perform resilience oversight, 325
key performance indicators (KPIs), 325
key risk indicators (KRIs)
defined, 975
performing resilience oversight, 325
Knowledge and Information Management (KIM)
access controls for information assets, 525–526
achieve specific goals, 533
assign responsibility for, 538–539
availability of information assets, 530–531
categorize information assets, 517–518
Cloud Computing and, 963
collect improvement information, 548–549
confidentiality and privacy considerations, 523–524
configuration management, 529
controls for information assets, 519–521
defined, 975
disposal management, 526–527
document organizational and intellectual knowledge of staff, 532–533
duplication and retention of information assets, 531–532
encrypt high-value information, 524–525
establish defined process for, 547–548
establish process governance, 534–536
FISMA compliance, 959
identify and assess risks, 522
identify and involve relevant stakeholders, 542–543
integrity management, 527
introductory notes, 513–514
manage work product configurations, 541
mitigate risks, 523
modification management, 527–528
monitor and control the process, 543–545
objectively evaluate adherence, 546
as Operations process area, 57
plan the process, 536
prioritize information assets, 516–517
protect information assets, 518–519
provide resources for, 536–538
purpose of, 513
related process areas, 514–515
resilience requirements for information assets, 519
review status with higher-level managers, 547
risk management and, 521
summary of specific goals and practices, 515
train people for, 540–541
validity and reliability of information assets, 529–530
knowledgebase for compliance data, 220
for incident management, 481
learning
from incidents and events, 493
integrating incident handling with problem management, 494–495
lessons learned and communicated, 639–640
overview of, 493
post-incident review, 493–494
translating lessons into strategy, 495–496
learning phase, process improvement, 82–83
legal issues. See laws
libraries, process asset, 613–614
licensing agreements, with external entities, 360–362
life-cycle
addressing resilience for software assurance, 104–110
of assets, 794
integration of resilience requirements in, 797
resilience of, 36–39
line of business, 976
Lockheed Martin Corporation, using CERT-RMM, 110–115
logs
asset modification, 883–884
configuration management, 887
Incident Management and Control, 480–481
MA. See Measurement and Analysis (MA)
maintenance
adaptive, 285, 966
of infrastructure, 190–191
perfective, 285, 979
preventive, 285, 979
of service continuity tests, 851
of technology assets, 894–895
manage work product configurations.
See work product configurations
managed process
as capability level 2, 70–72
defined, 976
management
developing operational resilience plan for, 314–316
identity. See identity management of risks due to external dependencies, 349–350
management, preparing for communications establish plan, 183–185
establish program, 185–186
identify and plan staff, 186–188
overview of, 183
management, preparing for compliance, establish guidelines and standards, 214
establish plan, 211–212
establish program, 212–214
overview of, 210–211
managers
identifying vital, 689
process governance and, 946
review with higher-level. See higher-level managers, reviewing with
Managing for Enterprise Security, (Caralli 2004), 11
maturity advantage, of CERT-RMM, 7
maturity models
CERT-RMM objectives vs., 12
CERT-RMM vs., 18–19
characteristics setting CERT-RMM apart from other, 113
raising bar on business resilience, 111–112
measurement. See also improvement information, collecting for assessing performance, 425–426
benefits of CERT-RMM, 5–7
effectiveness of service continuity plans, 851
establish corrective actions, 325–326
establish risk measurement criteria, 722–723
objectives, 976
of operational resistance, 115–118
perform resilience oversight, 324–325
repository, 612–613
Measures and Analysis (MA)
Access Management and, 170–171
achieve specific goals, 565
align activities with information needs and objectives, 553
analysis procedures for, 559–561
analyze measurement data, 562–563, 640
assign responsibility for, 569–570
collect improvement information, 576
collect measurement data, 561–562
communicate results, 564–565
data collection and storage procedures for, 557–559
defined, 976
establish defined process for, 575–576
establish objectives, 553–555
establish process governance, 566–567
identify and involve relevant stakeholders, 571–573
introductory notes, 551–552
manege work product configurations, 571
measurement results, 561
measures for, 556–557
measuring operational resistance using CERT-RMM, 115–118
monitor and control the process, 573–574
monitor asset definition and management process, 142–144
objectively evaluate adherence, 574–575
plan the process, 567
as Process Management, 59
provide resources for, 567–569
purpose of, 551
related process areas, 552
review status with higher-level managers, 573
store data and results, 563–564
summary of specific goals and practices, 552
train people for, 570–571
measurement results
analyze data, 562–563
collect data, 561–562
communicate, 564–565
overview of, 561
store data and results, 563–564
measures
base measures, 556, 561–562, 967
classes of commonly used, 612–613
defined, 976
derived measures, 556, 561–562, 963, 971
overview of, 556–557
media, distribution methods and, 593
Mehrvari, Dr. Nader, PhD, 109–110
memoranda of agreement, with external entities, 360–362
methods. See also tools, techniques, and methods
controls management, 261
environmental control, 295
establishing infrastructure for communications, 190–191
identify communications, 188–190
metrics. See also improvement information, collecting; monitor and control
capacity planning, 896
for high-value technology assets, 893
measure and assess performance with, 425–426
Measurement and Analysis, 551
for monitoring process, 602
for operational resistance, 117–118
performing resilience oversight, 324–325
mitigation
conflict mitigation plans, 755
for external dependencies, 352
for facility assets, 281–282
implement risk strategies, 731
risk mitigation plans, 729–731
of risks, 729
of staff risks, 692–693
technology asset risks, 880–881
model components. See components, model
model relationships
model view. See model view
objective views. See objective views, for assets
overview of, 53–54
model scope
asset scope, 89–90
defined, 84, 976
establishing improvement objective with, 87–88
practice-level scope, 88–89
resilience scope, 89–90
targeted improvement roadmaps, 88
model view
defined, 54
Engineering process areas, 56
Enterprise Management process areas, 54–55
Operations process areas, 56–57
Process Management, 57–59
model-based process improvement, using CERT-RMM for, 80–83
modification management, for information assets, 527–528
MON. See Monitoring (MON)
monitor and control
Access Management, 169–171
Asset Definition and Management, 142–144
Communications, 203–205
Compliance, 225–226, 236–237
controls for information assets, 521
Controls Management, 265–266
Enterprise Focus, 333–336
Environmental Control, 300–302
event detection and, 478–479
execution of software and system development plan, 810–812
External Dependencies
Management, 375–377
generic goals and practices, 951–953
Human Resource Management, 442–444
for identity changes, 455–456
monitor and control (contd.)
Identity Management, 468–470
Incident Management and Control, 506–508
Knowledge and Information Management, 543–545
Measurement and Analysis, 573–574
Monitoring, 601–603
Organizational Process Definition, 624–626
Organizational Process Focus, 649–650
Organizational Training and Awareness, 680–682
People Management, 711–713
performing resilience oversight, 324–325
process implementation and, 639
Resilience Requirements Development, 765–766
Resilience Requirements Management, 787–789
Resilient Technical Solution Engineering, 823–826
Risk Management, 741–743
risks to information assets, 522
Service Continuity, 862–864
software and systems, 795
Technology Management, 909–911
Vulnerability Analysis and Resolution, 937–939
Monitoring (MON)
achieve specific goals, 594
analyze and prioritize requirements for, 585–587
assign responsibility for, 597–598
collect and record information, 591–592
collect improvement information, 604–605
defined, 976
develop resilient software across life cycle with, 108
distribute information, 592–594
establish collection standards and guidelines, 589–591
establish defined process, 604
establish process governance, 594–595
establish requirements for, 583–585
establishing/maintaining program for, 578–581
establish/maintain infrastructure for, 588–589
FISMA compliance, 959
identify and involve relevant stakeholders, 581–582, 600–601
introductory notes, 577–578
manage work product configurations, 599–600
monitor and the control process, 601–603
objectively evaluate adherence, 603
plan the process, 596
as Process Management, 59
provide resources for, 596–597
purpose of, 577
related process areas, 578
relationships driving resilience at enterprise level, 55
relationships driving threat/incident management, 58
review status with higher-level managers, 603
summary of specific goals and practices, 578
train people for, 598–599
objectively evaluate adherence. See also adherence, objective evaluation of
objectives, measurement and analysis aligning needs by objectives, 553
establishing, 553–555
updating, 559
objectives, setting and communicating capability level targets, 90–92
model scope, 87–90
organizational objectives, 84–85
organizational scope, 83–85
overview of, 83–85
relating process needs to, 631
using CERT-RMM for strategic/operational, 78
objects, creating identities for. See Identity Management (IM)
obligeations, compliance analyzing, 217–218
assign responsibility for, 231–232
collect and validate compliance data, 219–221
demonstrate extent of satisfaction with, 221–223
developing plan for managing, 211–212
establish ownership for meeting, 218–219
evaluate adherence to, 238
identify and document, 213–217
monitor activities, 225–226
remediate areas of non-compliance, 223–225
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method, CERT, 10
off-budget request for funds, process for, 391
off-cycle request for funds, process for, 391
online references
CERT-RMM, 12
The Crosswalk, 13
developing resilient software across life cycle, 108–109
OPD. See Organizational Process Definition (OPD)
open borders, stress of managing globalization risks, 22–23
operational constraints, 976
operational controls, 242
operational environments
identifying vulnerabilities, 917–918
maintain environmental conditions, 285–286
manage dependencies on public infrastructure, 288–289
manage dependencies on public services, 287
overview of, 282–283
natural disasters
availability of technology assets and, 890–891
identifying staff risks, 691
NERC (North American Electric Reliability Corporation), 100, 102
non-compliance demonstrating extent of compliance obligation satisfaction, 221–223
evaluate adherence to compliance process, 238
remediate areas of, 223–225
requirements for identifying and documenting risks of, 214
North American Electric Reliability Corporation (NERC), 100, 102
notes, process area defined, 47–48
typographical and structural conventions, 51
notification communications, 187
numbering scheme, process areas, 47–49
objective views, for assets facilities, 60–61, 63–64
information, 59, 61
people, 59–60
perspectives addressed by, 59
technology, 60, 62
perform facility sustainability planning, 284–285
plan for facility retirement, 289–290
operational objectives
establish scope of improvement, 84
using CERT-RMM to support, 78
operational resilience, 976–977
operational resilience management
applying risk information to, 731–732
assets, 30–33
business processes, 29–30
CERT-RMM v1.1 introducing system of, 12
as competitive differentiator, xvi
defined, 105, 977
developing program for, 316–317
governing. See Enterprise Focus (EF)
identifying resilience requirements. See Resilience Requirements Development (RRD)
incident management and, 473–474
life-cycle coverage, 36–39
managing resilience requirements. See Resilience Requirements Management (RRM)
managing risk, 717
measuring using CERT-RMM, 115–118
monitoring and, 577, 583
resilience requirements, 33–35
services, 27–29
strategies for protecting/sustaining assets, 35–36
training and awareness and, 653
operational resilience process group (ORPG), 617, 672
operational resilience requirements
Access Management and, 153–156
asset disposal and, 526
for assets. See Resilience Requirements Development (RRD)
assign to technology assets, 875–876
change management, 131
Communications and, 179–181, 183–184
defined, 977, 982
driving operational resilience through, 33–35
establishing, 26–27
for facility assets, 276–277
identify inconsistencies in meeting, 778
for information assets, 518–519
maintain traceability of, 776–777
manage changes to, 775–776
Measurement and Analysis and, 554
obtain commitment to, 774–775
for software and system development, 797
for software and systems, 800–801
understanding, 773–774
operational risk
common problems of, 3–4
defined, 25–26, 977
how CERT-RMM solves problems of, 5–6
managing. See Risk Management (RISK)
overview of, 2–3
to technology assets, 878–881
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method, CERT, 10
Operations process areas
AM. See Access Management (AM)
defined, 7–8
EC. See Environmental Control (EC)
EXD. See External Dependencies Management (EXD)
IM. See Identity Management (IM)
IMC. See Incident Management and Control (IMC)
KIM. See Knowledge and Information Management (KIM)
model view of, 56–57
overview of, 42–43
PM. See People Management (PM)
TM. See Technology Management (TM)
VAR. See Vulnerability Analysis and Resolution (VAR)
OPE. See Organizational Process Focus (OPF)
optimization of resilience expenditures/investments
determining return on resilience investments, 396–397
identify cost recovery opportunities, 397–398
optimize resilience expenditures, 394–396
overview of, 394
organizational and intellectual knowledge, of staff, 532–533
organizational assets. See also Asset Definition and Management
creating identities for access to, 449–451
defined, 978
enable access to, 152–155
establish common understanding of, 126–128
establish ownership and custodianship, 128–130
establishing, 123–124
inventory assets, 124–126
manage and control access to, 151–152
returning upon departure from job, 430–431
organizational impact area. See area of impact
organizational objectives, 84–85
organizational process assets
establish measurement repository, 612–613
establish process asset library, 613–614
establish rules and guidelines for integrated teams, 615–616
establish work environment standards, 614–615
establishing, 608
set of standard processes, 608–610
 tailoring criteria and guidelines, 610–612
Organizational Process Definition (OPD)
Access Management and, 173–174
achieve specific goals, 617
assign responsibility for, 620–621
collect improvement information, 628
defined, 978
establish defined process, 627–628
establish measurement repository, 612–613
establish process asset library, 613–614
establish process governance, 617–618
establish rules and guidelines for integrated teams, 615–616
establish standard processes, 608–610
establish tailoring criteria and guidelines, 610–612
establish work environment standards, 614–615
identify and involve relevant stakeholders, 623–624
introductory notes, 607
manage work product configurations, 623
monitor and control the process, 624–626
objectively evaluate adherence, 626–627
plan the process, 619
as Process Management, 59
provide resources for, 619–620
purpose of, 607
related process areas, 608
review status with higher-level managers, 627
Organizational Process Definition (OPD) (contd.)
summary of specific goals and practices, 608
train people for, 621–623
Organizational Process Focus (OPF)
Access Management and, 173–174
achieve specific goals, 641
appraise organizational processes, 632–633
Asset Definition and Management, 145
assign responsibility for, 645–646
collect improvement information, 652
deploy process assets, 636–637
deploy standard processes, 638
determine process improvement opportunities, 630
establish defined process, 652
establish process action plans, 634–635
establish process governance, 641–643
establish process needs, 631–632
identify and involve relevant stakeholders, 648–649
identify improvements to processes, 633–634
implement process action plans, 636
incorporate experiences into process assets, 639–641
introductory notes, 629–630
manage work product configurations, 647–648
monitor and control the process, 649–650
monitor process implementation, 639
objectively evaluate adherence, 651
plan and implement process actions, 634
plan the process, 643
as Process Management, 59
provide resources for, 643–645
purpose of, 629
review status with higher-level managers, 651
summary of specific goals and practices, 630
train people for, 646–647
organizational process maturity, 978
organizational scope defined, 978
overview of, 84–87
organizational sensitivity. See sensitivity
organizational subunits defined, 978
in organizational scope, 86
planning practice instantiation, 96
organizational superunits defined, 979
in organizational scope, 86
planning practice instantiation, 96
Organizational Training and Awareness (OTA)
Access Management and, 164, 167
achieve specific goals, 671
assess effectiveness of awareness program, 662–663
assess effectiveness of training program, 670–671
Asset Definition and Management and, 137, 140
assign responsibility for, 676–677
collect improvement information, 684
collect improvement information, 684
conduct training, 668
defined, 979
deliver resilience training, 668–669
Enterprise Management and, 54–55
establish awareness delivery capability, 658–660
establish awareness needs, 655–657
establish awareness plan, 657–658
establish defined process for, 683
establish process governance, 671–673
establish training capability, 666–668
establish training needs, 664–665
establish training plan, 665–666
establish training records, 669–670
FISMA compliance, 960
identify and involve relevant stakeholders, 679–680
Incident Management and Control and, 310–311
introductory notes, 653–654
Knowledge and Information Management and, 548–549
manage work product configurations, 678–679
Measurement and Analysis and, 576
monitor and control the process, 680–682
Monitoring and, 604–605
objectively evaluate adherence, 682–683
Organizational Process Definition and, 628
Organizational Process Focus and, 652
perform awareness activities, 660–661
perform awareness records, 661–662
plan the process, 673–674
provide resources for, 674–675
purpose of, 653
related process areas, 654
review status with higher-level managers, 683
summary of specific goals and practices, 655
train people for, 677–678
organizational units defined, 979
deploying standard processes to, 638
in organizational scope, 85–87
planning practice instantiation, 96
standard processes tailored by, 607–608
organizationally high-valued services.
See high-value services
organizations defined, 977
process asset library. See process asset library
role in External Dependencies
Management, 341–343
standard processes. See standard processes
ORPG (operational resilience process group), 617, 672
OTA. See Organizational Training and Awareness (OTA)
overhead allocation, funding resilience activities, 391
oversight, resilience
establish corrective actions, 325–326
as governance focus area, 322–323
for operational resilience management program, 317
overview of, 321
performing, 323–325
ownership
of access management, 152, 156, 168–169
of asset definition and management, 126–130
of compliance, 231–232
of compliance obligations, 218–219
defining, 32–33
of environmental control, 296–297
planning and, 946
P
partnerships, operational resilience management and, 2
passwords, access control via, 525
patch management, 889
PDCA (Plan, Do, Check, Act) cycle, 80–81, 82–83
peer pressure, 101–103
people
as asset. See Asset Definition and Management (ADM), People Management (PM), and Human Resource Management (HRM)
as asset in CERT-RMM, 31–32
policies (contd.)
Human Resource Management, 434–435
identify compliance obligations, 213–216
Identity Management, 461–462
Incident Management and Control, 498
information assets, 518
internal control, 241–242
Knowledge and Information Management, 535
Measurement and Analysis, 567
Monitoring, 595
Organizational Process Definition, 618
Organizational Process Focus, 642–643
Organizational Training and Awareness, 673
People Management, 702–703
release management, 889–890
Resilience Requirements Development, 758
Resilience Requirements Management, 780
Resilient Technical Solution Engineering, 815
Risk Management, 735
Service Continuity, 854–855
sponsoring resilience, 320–321
standard processes adhering to, 610
Technology Management, 901
Vulnerability Analysis and Resolution, 930
post-incident review, 493–494, 979
practice-level scope, 88–90
practices
damage of evaluation based on, 9–10
defining CERT-RMM, 14–15
generic. See generic goals and practices
limitations of organizations focused on, 9
organizing structure for deployed, 79–80
planning instantiation of, 95–96
pre-employment verification of staff, 418–419
preventive controls, 247–248
preventive maintenance defined, 979
of environmental conditions, 285
prioritization
of candidates for process improvement, 634
of control objectives, 246
of data collection/storage, 559
of external dependencies, 348–349
of high-value services, 835–836
of information assets, 516–517
of measures, 557
of monitoring requirements, 585–587
of risk, 727
of risks, 726
of staff, 687
of vulnerabilities, 924–925
prioritization of technology assets defined, 979
of information assets, 523–524
privileges. See access privileges
problem management defined, 980
integrating incident handling with, 494–495
procedures
as critical dimension of organizations, 8–9
for handling information assets, 517
process actions
establish action plans, 634–635
implement action plans, 636
planning and implementing, 634
process architecture, 610, 980
process areas
ADM. See Asset Definition and Management (ADM)
AM. See Access Management (AM)
arranging in model view, 54–59
by category, 41–42
in CERT-RMM and CMMI models, 12–15
COMM. See Communications (COMM)
COMP. See Compliance (COMP)
component categories, 42–44
component descriptions, 44–47
CTRL. See Controls Management (CTRL)
defined, 980
EC. See Environmental Control (EC)
EF. See Enterprise Focus (EF)
EXD. See External Dependencies Management (EXD)
FRM. See Financial Resource Management (FRM)
generic goals and practices, 950
HRM. See Human Resource Management (HRM)
icons, 42–43
IM. See Identity Management (IM)
IMC. See Incident Management and Control (IMC)
institutionalization of. See institutionalization
KIM. See Knowledge and Information Management (KIM)
MA. See Measurement and Analysis (MA)
MON. See Monitoring (MON)
numbering scheme, 47–49
OPD. See Organizational Process Definition (OPD)
OPF. See Organizational Process Focus (OPF)
OTA. See Organizational Training and Awareness (OTA)
PM. See People Management (PM)
RISK. See Risk Management (RISK)
RRD. See Resilience Requirements Development (RRD)
RRM. See Resilience Requirements Management (RRM)
RTSE. See Resilient Technical Solution Engineering (RTSE)
SC. See Service Continuity (SC)
supporting generic practices, 74–75
tags, 47–49
TM. See Technology Management (TM)
typographical and structural conventions, 49–51
VAR. See Vulnerability Analysis and Resolution (VAR)
process asset library
collecting improvement information for communications, 208
defined, 977, 980
establishing, 613–614
process capability, 980
process element, 980
process governance. See governance, process
process improvement
appraisal of organizational processes, 632–633
CERT-RMM for, 77
CERT-RMM for model-based, 80–83
CERT-RMM vs. CMMI focus, 15
determining opportunities for, 630
establish organizational process needs, 631–632
identify improvements, 633–634
proposals, 641
Process Management process areas defined, 7–8
MA. See Measurement and Analysis (MA)
model view of, 37–59
MON. See Monitoring (MON)
OPD. See Organizational Process Definition (OPD)
OPF. See Organizational Process Focus (OPF)
overview of, 42–43
process maturity, 978
process performance, 980
processes
  defined, 980
  definition of. See Organizational Process Definition (OPD)
  focus of. See Organizational Process Focus (OPF)
production environment, use of CERT-RMM in, 14
profiles, identity
  assigning roles to identities, 454
  correcting inconsistencies in, 458–459
  deprovisioning, 459–460
  establishing, 450–451
  establishing identity community from, 452–453
  plan process for, 462–463
protection, of information assets
  controls for, 519–521
  overview of, 518–519
  resilience requirements, 519
protection, of technology assets
  controls for, 876–878
  overview of, 874–875
  resilience requirements, 875–876
protection strategy
  for assets, 35–36
  defined, 981
  resilience requirements as basis of, 35
protocols, communication, 491
provide resources, generic goals and practices. See resources, providing
provisioning
  defined, 981
  establishing identities and, 447
  proximity, 981
public infrastructure, 981
public services
  defined, 981
  managing dependencies on, 287
purchase orders, with external entities, 360–362
purchase requests, funding resilience activities, 391
purpose statements
  for process areas, 44, 48
  typographical and structural conventions, 50
Q
quality attributes, in software and system development, 793–794
questionnaires, for assessing effectiveness of awareness program, 662
R
reassignment, of roles and responsibilities, 429
records
  of awareness activities, 661–662
  identify vital organizational, 837–839
  of maintenance operations, 895
  of monitoring information, 591–592
  of training activities, 669–670
recovery plans, service continuity and, 839
recovery point objectives (RPOs)
  availability of technology assets and, 892–893
  defined, 981
recovery time objectives (RTOs)
  availability of technology assets and, 892–893
  defined, 981
redundancy
  availability of technology assets and, 891
  establish for vital staff, 694–695
  succession planning and, 695–697
references, process area
  defined, 47–48
  typographical and structural conventions, 51
registration, of identities, 450–451
  regulations defined, 981
  documenting events and, 481–482
  electric power industry and, 101–103
  establish scope of improvement, 84
  managing. See Compliance (COMP)
  stress of managing operational risk, 23
related process areas section, 45, 48
relationships
  establish enterprise specifications, 353–354
  establish formal agreements, 360–362
  establish resilience specifications, 355–357
  evaluate/select external entities, 358–359
  identify internal and external dependencies and interdependencies, 837
  model view. See model view objective view. See objective views, for assets
  overview of, 53–54, 352–353
  between process elements, 610
release builds, 981
release management
  defined, 981
  technical solutions released into production, 812–813
for technology assets, 889–890
reliability
  of information assets, 529–530
  resilience and, 100–101
remediation
  of areas of non-compliance, 223–225
  identifying areas needing compliance, 223
repeatability, of measures, 557
reports
  on communications effectiveness, 194
  on compliance obligation satisfaction, 222–223
  on corrective actions, 326
  on event status, 483
  external dependencies management, 362
  in incident management, 478–479, 486
  on incident status, 491
  logged events and, 481
  post-incident review, 494
  on resilience oversight, 325
repositories
  for compliance data, 220–221
  identity repository, 452, 974
  for processes and work products, 955
  for skills, 985
  for vulnerability information, 922–923, 925, 987
required components
  defined, 981
  overview of, 43–44
  summary of, 48
requirements
  guidelines for Resilient Technical Solution Engineering, 800–801
  validate service continuity plans against, 845–846
requirements, for Monitoring
  analyze and prioritize, 585–587
  establishing, 583–589
requirements, resilience
  developing. See Resilience Requirements Development (RRD)
  managing. See Resilience Requirements Management (RRM)
  operational. See operational resilience requirements
repositories
  Requirements Development, CMMI process area, 795
  residual risk, 981
resilience
configuration management and, 884–885
defined, 981, xv
establish resilience-focused technology assets, 873–874
identifying vital resilience functions of staff, 689
inserting obligations in job descriptions, 423
management. See operational resilience management
reliability and resilience in, 100–101
requirements. See operational resilience requirements
resilience-aware culture, 319–320
resilience-focused assets, 275
scope, 89–90
of service, 14
staff and training, 982
using goals and objectives to support, 423–424
resilience budgets
defined, 982
establishing, 388–389
funding resilience activities, 391
resolving funding gaps, 388–389
Resilience Requirements Development
(RRD)
achieve specific goals, 756
analyze resilience requirements, 755
assign enterprise resilience requirements to services, 753–754
assign responsibility for, 760–761
Cloud Computing and, 962
collect improvement information, 769
define required functionality, 754–755
defined, 982
develop service requirements, 752
developing resilient software across life cycle with, 107
as Engineering process area, 56
establish asset resilience requirements, 752–753
establish defined process for, 768–769
establish process governance, 757–758
for facility asset resilience requirements, 276–277
FISMA compliance, 960
identify and involve relevant stakeholders, 763–764
identify enterprise requirements, 750–752
introductory notes, 747–750
manage work product configurations, 763
monitor and control process of, 765–766
objectively evaluate adherence, 767
plan the process, 758–759
provide resources for, 759–760
purpose of, 747
related process areas, 750
review status with higher-level managers, 768
summary of specific goals and practices, 750
train people for, 761–763
validate resilience requirements, 756
Resilience Requirements Management
(RRM)
achieve specific goals, 778
assign responsibility for, 782–783
Cloud Computing and, 962
collect improvement information, 791–792
defined, 982
developing resilient software across life cycle, 107
as Engineering process area, 56
establish defined process for, 791
establish process governance, 779–780
identify and involve relevant stakeholders, 786–787
identify inconsistencies in meeting resilience requirements, 778
introductory notes, 771–772
maintain traceability of resilience requirements, 776–777
manage changes to resilience requirements, 753–776
manage work product configurations, 785–786
managing change to resilience requirements, 131
monitor and control the process, 787–789
objectively evaluate adherence, 789–790
obtain commitment to resilience requirements, 774–775
plan the process, 780–781
provide resources for, 781–782
purpose of, 771
related process areas, 772
review status with higher-level managers, 790–791
summary of specific goals and practices, 772
train people for, 783–785
understanding resilience requirements, 773–774
resilience specifications
defined, 982
evaluating/selecting external entities based on, 358–359
for external dependencies, 355–357
external dependencies management, 361
resilience training
delivery of, 668–669
establish training needs, 664–665
establish training plan, 665
materials, 666–667
Resilient Technical Solution
Engineering (RTSE)
achieve specific goals, 813
assign responsibility for, 818–819
collect improvement information, 828–829
create development plans for resilient technical solutions, 807–808
defined, 982
developing resilient software across life cycle, 106–107
as Engineering process area, 56
establish defined process for, 827–828
establish process governance, 814–815
identify and involve relevant stakeholders, 822–823
identify architecture and design guidelines, 801–802
identify assembly and integration guidelines, 805–807
identify general guidelines, 798–800
identify implementation guidelines, 802–805
identify requirements guidelines, 800–801
influenced by CMMI process areas, 108
integrating selected guidelines with software and system development process, 809–810
introductory notes, 793–796
manage work product configurations, 821–822
monitor and control the process, 823–826
monitoring execution of development plan, 810–812
objectively evaluate adherence, 826–827
plan the process, 816
provide resources for, 816–818
purpose of, 793
related process areas, 796
release solutions into production, 812–813
review status with higher-level managers, 827
select and tailor guidelines, 808–809
summary of specific goals and practices, 796
train people for, 820–821
resource needs, establishing
address skill deficiencies, 416–418
establish baseline competencies, 414–415
inventory skills and identify gaps, 415–416
overview of, 413
resources, providing. See also Financial Resource Management (FRM)
Access Management, 163–165
Asset Definition and Management, 137–138
Communications, 197
Compliance, 213, 229–231
Controls Management, 259–260
Enterprise Focus, 328–330
Environmental Control, 293–295
External Dependencies
Management, 368–370
Financial Resource Management, 400–402
generic goals and practices, 948
Human Resource Management, 436–437
Identity Management, 462–464
Incident Management and Control, 490–500
Knowledge and Information Management, 536–538
Measurement and Analysis, 567–569
Monitoring, 596–597
Organizational Process Definition, 619–620
Organizational Process Focus, 643–645
Organizational Training and Awareness, 674–675
People Management, 704–706
Resilience Requirements Development, 759–760
Resilience Requirements Management, 781–782
Resilient Technical Solution Engineering, 816–818
Risk Management, 736–737
Service Continuity, 856–857
Technology Management, 902–904
Vulnerability Analysis and Resolution, 931–932
responding to incidents declare events for response planning, 483–484
limiting organizational impact of incidents, 488–490
recovery and, 487
response and recovery, responding to incidents, 487
responsibilities. See also roles incident management plan and, 477–478
linking to identity. See Identity Management (IM)
in organizational identity, 448
periodic review to identify invalid identities, 457
roles vs., 453
responsibilities, assigning
Access Management, 165–166
Asset Definition and Management, 138–139
Communications, 199–200
Compliance, 231–232
Controls Management, 261–262
Enterprise Focus, 330–331
Environmental Control, 296–297
External Dependencies
Management, 370–371
Financial Resource Management, 402–403
generic goals and practices, 948–949
Human Resource Management, 437–438
Identity Management, 464–465
Incident Management and Control, 501–502
Knowledge and Information Management, 338–339
managing changes to employment status, 429
Measurement and Analysis, 569–570
Monitoring, 597–598
Organizational Process Definition, 620–621
Organizational Process Focus, 645–646
Organizational Training and Awareness, 676–677
People Management (PM), 706–707
Resilience Requirements Development, 760–761
Resilience Requirements Management, 782–783
Resilient Technical Solution Engineering, 818–819
Risk Management, 737–738
Service Continuity, 857–858
Technology Management, 904–905
Vulnerability Analysis and Resolution, 933
restoration plans
incident response and, 489
service continuity and, 839
restrictions. See access privileges retention, of information assets, 531–532
retirement, develop plan for facility, 289–290
retrieval, of compliance data, 220
return on resilience investment (RORI) calculation, 396–397
defined, 983
review status with higher-level managers, generic goals and practices, 953
reviews
with high-level managers. See higher-level managers, reviewing with monitoring and controlling
and, 952
of monitoring processes, 602–603
in objective evaluation of adherence, 953
periodic of environmental control process, 302
periodic of identities, 456–457
post-execution review of service continuity plans, 851
sources of vulnerability, 921
revision history, in change management, 888
RISK. See Risk Management (RISK)
risk assessing controls for, 253, 257
assessment of facility asset, 280–281
availability of technology assets and, 892
controlling operational environment, 282–283
defined, 983
defining controls for, 248–250
due to external dependencies, 349–350
governance, xvi
identifying and assessing external, 350–351
identifying related to involuntary terminations, 432
mitigation strategies for external dependencies, 352
mitigation strategies for facility assets, 281–282
of non-compliance, 222
protecting information assets and, 518–519
service continuity planning and, 832
risk analysis, 983
risk appetite, 983
risk category, 983
risk disposition
assigning, 727–729
defined, 983
risk management
focus on high-value services, 836
incident management and, 475
interoperability and, 898–899
risk management, for information assets
identify and assess risks, 522
mitigate risks, 523
risk management, for information assets (contd.)
overview of, 521
prioritization and, 515–517
risk management, for technology assets
identify and assess risks, 879–880
mitigate risks, 880–881
overview of, 878–879
prioritization of technology assets, 871
risk management, of staff risk
identify and assess staff risks, 691–692
mitigate staff risks, 692–693
overview of, 691
Risk Management (RISK)
achieve specific goals, 733
apply risk information to operational resilience management, 731–732
assign responsibility for, 737–738
assign risk disposition, 727–729
categorize and prioritize risks, 727
Cloud Computing and, 962
collect improvement information, 743–746
define risk parameters, 721–722
defined, 983
determine sources and categories of risk, 719–720
develop risk mitigation plans, 729–731
Enterprise Management, 54–55
establish defined process for, 744–745
establish operational risk management strategy, 720–721
establish process governance, 734–735
establish relationship between assets and services, 130
establish risk measurement criteria, 722–723
evaluate risks, 726–727
FISMA compliance, 960
identify and involve relevant stakeholders, 740–741
identify asset-level risks, 723–725
identify service-level risks, 725–726
implement risk strategies, 731
insider threats and, 964
introductory notes, 717–718
manage work product configurations, 740
mitigate risks, 729
monitor and control the process, 741–743
objectively evaluate adherence, 743–744
plan the process, 735
preparing for, 719
provide resources for, 736–737
purpose of, 717
related process areas, 718
relationships driving threat/incident management, 58
review and adjust risk-related strategies, 732–733
review status with higher-level managers, 744
summary of specific goals and practices, 718
train people for, 738–739
risk measurement criteria, 983
risk mitigation
defined, 983
for external dependencies, 352
for facility assets, 281–282
of general risks, 729
implementing process action plans, 731
risk mitigation plans, 729–731, 983
of staff risks, 692–693
of technology asset risks, 880–881
risk parameters, 984
risk statements
defined, 984
developing, 725
staff risks and, 692
risk taxonomy, 984
risk threshold, 984
risk tolerance
defined, 984
overview of, 721–722
vulnerability analysis and resolution strategy and, 918–919
roles. See also responsibilities
access privileges and, 153–156
assign for knowledge and information management, 539
assign to identities, 453–454
identifying vital staff and, 688
incident management plan and, 477–478
linking to organizational identity. See Identity Management (IM)
managing changes to employment status, 429
organizational process definition process, 621
periodic review to identify invalid identities, 457
root-cause analysis
applying to vulnerabilities, 927–928
defined, 984
in post-incident review, 494
RORI (return on resilience investment) calculation, 396–397
defined, 983
RPOs (recovery point objectives)
availability of technology assets and, 892–893
defined, 981
RRD. See Resilience Requirements Development (RRD)
RRM. See Resilience Requirements Management (RRM)
RTOs (recovery time objectives)
availability of technology assets and, 892–893
defined, 981
RTSE. See Resilient Technical Solution Engineering (RTSE)
rules, establish for integrated teams, 615–616
S
safety, work environment standards, 613
SC. See Service Continuity (SC)
scalability, of CERT-RMM, 15
SCAMPI (Standard CMMI Appraisal Method for Process Improvement), 92
scope
of assets and environments, 917–918
basing improvement objectives on, 84–85
capability appraisal and, 93–94
CERT-RMM, 14
of control assessment, 255–256
defined, 984
model scope, 87–90, 976
organizational scope, 84–87, 978
of risk assessment, 281
RORI calculation, 396–397
scorecard, governance, 324
screening, pre-employment, 418–419
secure design pattern, 984
security
benefits of CERT-RMM, 5
evolution of CERT-RMM, 10–11
protection of information assets, 518–519
protection of technology assets, 874–875
protection strategy, 35–36
service continuity plans, 843–844
work environment standards, 615
SEI (Software Engineering Institute), 8, 9–12
sensitivity
asset disposal and, 526
attributes of information assets, 514
categorize information assets by, 517–518
defined, 984
identifying staff responsible for sensitive assets, 690
organizational sensitivity, 978
service continuity plans
assign staff to, 842–843
availability of technology assets and, 891–893
defined, 985
develop and document, 840–842
develop testing program and standards for, 847–848
develop training for, 844
establish change criteria for, 852
evaluate test results, 849–850
execute, 850–851
exercise tests of, 849
identify and resolve conflicts in, 846
identify and involve relevant stakeholders, 860–862
identify and resolve conflicts in plans, 846
identify communications requirements with, 180–181
identify high-value services, 835–836
identify internal and external dependencies and interdependencies, 837
identify required plans, 840
identify vital organizational records and databases, 837–839
incident response and, 489
introductory notes, 831–832
maintain changes to plans, 852–853
maintain plans, 851
manage work product configurations, 860
measure effectiveness of, 851
prepare for staff redeployment, 697–698
return-to-work plan, 700
risk mitigation and, 733
store and secure, 843–844
support of staff during disruptive events, 699
technology assets in, 873
validation of, 845–846
Service Continuity (SC)
achieve specific goals, 853
assign responsibility for, 837–838
assign staff to plans, 842–843
Cloud Computing and, 963
collect improvement information, 866–867
controls management using, 243 defined, 984
develop and document plans, 840–842
develop and document test plans, 848
develop operational resilience management plan, 315–316
develop resilient software across life cycle with, 108
develop testing program and standards, 847–848
develop training, 844
as Engineering process area, 56
establish change criteria, 852
establish defined process for, 865–866
establish process governance, 853–855
establish resilience-focused facility assets, 275
establish standards and guidelines for, 835
evaluate test results, 849–850
execute plans, 850–851
FISMA compliance, 960
identify and involve relevant stakeholders, 860–862
identify and resolve conflicts in plans, 846
identify communications requirements with, 180–181
identify high-value services, 835–836
identify internal and external dependencies and interdependencies, 837
identify required plans, 840
identify vital organizational records and databases, 837–839
incident response and, 489
introductory notes, 831–832
maintain changes to plans, 852–853
maintain plans, 851
manage work product configurations, 860
measure effectiveness of plans, 851
monitor and control the process, 862–864
objectively evaluate adherence, 864–865
plan the process, 855
prepare and plan for, 833–835
protect and sustain services and assets, 131
provide resources for, 856–857
purpose of, 831
related process areas, 832–833
relationships driving threat/incident management, 58
review status with higher-level managers, 865
store and secure plans, 843–844
summary of specific goals and practices, 833
test (exercise) plans, 849
train people for, 858–859
validate plans, 845–846
service disruption, 915
service level agreements (SLAs), 985
service profiles, 985
service-level controls
assessing effectiveness of, 253–254
defining, 248–250
service-level resilience requirements analyze and validate, 754
assigning enterprise resilience requirements to services, 753–754
defined, 985
developing, 752
overview of, 748
service-level risks
identifying, 725–726
review and adjust strategies for, 732–733
services
in CERT-RMM, 14
CERT-RMM not establishing, delivering or managing, 14
concept of, 27–29
defined, 984
establish relationship between assets and, 130–131
focus on high-value, 29
fueled by assets, 30–33
life-cycle of, 38–39
operational risk objectives, 25–27
prioritize external dependencies relative to, 348–349
prioritize information assets relative to, 516
services map, 753
service-support staff, 689
shared resilience requirements, 985
Shewhart cycle, 80
silos, 5
skills
addressing gaps and deficiencies, 416–417
identifying gaps and deficiencies, 416
incident management plan and, 477–478
inventory or repository, 413–416, 985
service continuity plans and, 844
training needs and, 665
skills, training
Access Management, 167
Asset Definition and Management, 138, 140
Communications, 200–201
Compliance, 232–233
Controls Management, 262–263
Enterprise Focus, 331
Environmental Control, 297–298
External Dependencies Management, 371–372
Financial Resource Management, 403–404
generic goals and practices, 949–950
Human Resource Management, 439–440
Identity Management, 465–466
Incident Management and Control, 502–503
Knowledge and Information Management, 537, 540–541
Measurement and Analysis, 570–571
Monitoring, 599
Organizational Process Definition, 622
Organizational Process Focus, 646–647
Organizational Training and Awareness, 677–678
People Management, 708–709
Resilience Requirements Development, 762–763
Resilience Requirements Management, 784–785
Resilient Technical Solution Engineering, 820–821
Risk Management, 739
Service Continuity, 859
staff, training (contd.)
Technology Management, 906
Vulnerability Analysis and Resolution, 934
SLAs (service level agreements), 985
sociopolitical events, controlling operational environment, 283
software
architecture and design guidelines, 801–802
assembly and integration guidelines, 805–807
errors, 891
execution of development plan, 810–812
implementation guidelines, 802–805
integrating selected resilience guidelines with development process for, 809–810
integrity of, 882
monitoring, 795
releasing resilient solutions into production, 812–813
resilience guidelines, 800–801
resilience requirements, 793–794
stress of managing as intangible asset, 22
tailoring resilience guidelines using selection criteria, 808–809
software assurance, using CERT-RMM
about the authors, 104–105
defined, 105
overview of, 105–110
Software Engineering Institute (SEI), 8, 9–12
specific goals and practices
defined, 45–46, 48, 985
tags and numbering scheme for, 49
typographical and structural conventions, 50
using practice-level scope, 88–89
sponsorship. See also managers, review with higher-level
commit funding for operational resilience management, 383–384
for compliance program, 214, 231
establish scope of improvement, 84–85
of identity, 451
sponsorship, for operational resilience management
commit funding, 318–319
overview of, 317–318
promote resilience-aware culture, 319–320
standards and policies, 320–321
staff
access controls for, 883–884
acquisition of, 418
assigning to service continuity plans, 842–843
defined, 985
document organizational and intellectual knowledge of, 532–533
establish vital, 687–690
incident response and, 490
for maintenance operations, 894–895
managing. See People Management (PM)
for operational resilience management program, 316–317
personnel services. See Human Resource Management (HRM)
post-incident review, 494
providing for incident closure, 492
resource provision and, 948
training. See training people
training in discovery of vulnerabilities, 923
verifying suitability of candidates, 418–419
staff, providing
Access Management, 163–164
Asset Definition and Management, 137
Communications, 186–188, 198–200
Compliance, 229–230
Controls Management, 260
Enterprise Focus, 329
Environmental Control, 293–294, 296–297
External Dependencies Management, 368–370
Financial Resource Management, 400–401
Human Resource Management, 436
Identity Management, 462–464
Incident Management and Control, 477–478, 499–500
Knowledge and Information Management, 537
Measurement and Analysis, 568
Monitoring, 596–597
Organizational Process Definition, 619–620
Organizational Process Focus, 644
Organizational Training and Awareness, 674
People Management, 704–705
Resilience Requirements Development, 759–760
Resilience Requirements Management, 781
Resilient Technical Solution Engineering, 817
Risk Management, 736–737
Service Continuity, 856
Technology Management, 902–903
Vulnerability Analysis and Resolution, 931–932
staff availability
establish redundancy for vital staff, 694–695
managing, 693–694
perform succession planning, 695–697
plan for return-to-work following disruptive events, 700–701
plan to support staff during disruptive events, 698–700
prepare for redeployment, 697–698
staff risks
identify and assess, 691–692
mitigate, 692–693
overview of, 691
stakeholders
communicating measurement results to, 564–565
communicating to regarding incidents, 489
defined, 985
distributing collected information to, 592–593
escalation of incidents for input from, 487–488
in monitoring processes, 581–582
for performing resilience oversight, 324–325
stakeholders, identify and involve
Access Management, 168–169
Asset Definition and Management, 141–142
Communications, 177–181, 202–203
Compliance, 234–236
Controls Management, 264–265
Enterprise Focus, 332–333
Environmental Control, 299–300
External Dependencies Management, 373–374
generic goals and practices, 951
Human Resource Management, 441–442
Identity Management, 467–468
Incident Management and Control, 504–506
Knowledge and Information Management, 542–543
Measurement and Analysis, 571–573
Monitoring, 600–601
Organizational Process Definition, 623–624
Organizational Process Focus, 648–649
Organizational Training and Awareness, 679–680
People Management, 710–711
Resilience Requirements
Development, 763–764
Resilience Requirements
Management, 786–787
Resilient Technical Solution
Engineering, 822–823
Risk Management, 740–741
Service Continuity, 860–862
Technology Management, 907–908
Vulnerability Analysis and
Resolution, 933–936
Standard CMMI Appraisal Method for
Process Improvement (SCAMPI), 92
standard processes
composition of, 607
defined, 978, 986
defined processes compared
with, 954
deploying, 638
establishing, 608–610
measurement repository for, 612
monitoring implementation of, 639
tailoring and, 611–612
standards. See also guidelines
for communications, 181–184
Compliance, 214
for configuration management, 886
establishing standard processes,
608–610
interoperability, 898
managing, See Compliance (COMP)
for monitoring, 589–591
for service continuity, 835
sponsoring resilience, 320–321
test service continuity plans against,
847–848
validate service continuity plans against,
845–846
for work environments, 614–615
statistics, descriptive statistics in data
analysis, 560
Stevens, James, 99–100
storage
of compliance data, 220
of data, 563–564
data collection and, 557–559
of service continuity plans, 843–844
strategic planning
defined, 986
developing operational resilience
management plan, 314–316
establish critical success factors,
310–312
establish organizational services,
312–314
establish scope of improvement, 84
establishing, 309–310
funding operational resilience
management, 383–384
performing resilience oversight for,
323–324
using CERT-RMM to support, 78
strategies
establish operational risk
management strategy, 720–721
establish vulnerability analysis and
resolution strategy, 918–920
implement risk strategies, 731
for protecting/sustaining assets,
35–36
review and adjust asset-level risk
strategies, 732
review and adjust service-level risk
strategies, 732–733
for staff redundancy, 695
translating lessons into, 495–496
strengths and weaknesses, appraisal of
organization, 632–633
stress
causes of in operational resilience
management, 2
CERT-RMM control of
organizational behavior
during, 21–23
managing operational resilience,
25–27
structural conventions, process areas,
49–51
subpractices, process area
defined, 47–48
typographical and structural
conventions, 51
subprocesses, 986
succession planning
defined, 986
perform, 695–697
summary of specific goals and
practices, process areas, 45
Supplier Management, Operations, 57
suppliers, 986
surveys
assess effectiveness of awareness
program, 662
assess effectiveness of training
program, 670
sustain
defined, 986
facility assets, 284–285
information, 35–36
services and assets, 131
technology assets, 891–894
sustainability planning, 285–286
Sustaining Operational Resiliency: A
Process Improvement Approach to
Security Management (Caralli
2006), 12
systems
architecture and design guidelines,
801–802
assembly and integration
guidelines, 805–807
execution of development plan,
810–812
implementation guidelines, 802–805
integrating selected resilience
guidelines with development
process for, 809–810
monitoring, 795
releasing resilient solutions into
production, 812–813
resilience guidelines, 800–801
resilience requirements, 793–794
tailing resilience guidelines using
selection criteria, 808–809
T
tag, process area, 47–49, 50
targeted improvement profile (TIP)
capability level ratings overlaid on,
93–94
overview of, 91–92
targeted improvement roadmaps (TIRs)
for achieving FISMA compliance,
957–961
for Cloud Computing, 961–963
establishing improvement objective
with, 88
for managing insider threats, 963
teams, establish rules and guidelines
for integration of, 615–616
technical controls
defined, 986
at enterprise/service/asset levels,
248–250
for facility assets, 277–279
for information assets, 519–521
overview of, 246–247
for technology assets, 876–878
technical solutions. See Resilient
Technical Solution Engineering
(TTSE)
Technical Solutions, CMMI process
area, 795
techniques. See tools, techniques, and
methods
technology. See also Asset Definition
and Management (ADM) and
Technology Management (TM)
access privileges focusing on, 153
as asset in CERT-RMM, 31–32
assets, 986
identity management and, 448–449
interoperability. See interoperability
life-cycle of, 37
managing operational risk of, 23
objective views for, 60, 62
operational resilience management
and, 2
protecting and sustaining, 35–36
resilience requirements for, 33–35
stress of managing operational risk
of, 22
as traditional focus of operational
risk management, 8–9
Technology Management (TM)
- access controls for, 882–883
- achieve specific goals, 899
- assign resilience requirements, 873–876
- assign responsibility for, 904–905
- Cloud Computing and, 962–963
- collect improvement information, 913–914
- defined, 986
- developing resilient software across life cycle with, 108
- establish and implement controls, 876–878
- establish defined process, 912–913
- establish process governance, 899–901
- establish resilience-focused technology assets, 873–874
- FISMA compliance, 961
- identify and assess risks, 879–880
- identify and involve relevant stakeholders, 907–908
- introductory notes, 869–870
- maintain technology assets, 894–895
- manage availability of technology assets, 890–891
- manage integrity of technology assets, 881–882
- manage risks, 878–879
- manage technology capacity, 893–897
- manage technology interoperability, 897–899
- manage work product configurations, 906–907
- mitigate risks, 880–881
- monitor and control, 909–911
- objectively evaluate adherence, 911–912
- as Operations process area, 57
- perform change management, 887–888
- perform configuration management, 883–887
- perform release management, 889–890
- plan the process for, 901–902
- prioritize technology assets, 871–873
- protect technology assets, 874–875
- provide resources for, 902–904
- purpose of, 869
- related process areas, 870
- review status with higher-level managers, 912
- summary of specific goals and practices, 870–871
- sustain technology assets, 891–894
- train people for, 905–906
- termination, external dependencies management, 362
- termination of employment involuntary, 428
- managing impact of position changes, 428–429
- managing involuntary, 431–432
- voluntary, 427
terms and conditions of employment, establishing, 420–422
test (exercise) service continuity plans develop and document tests, 848
- develop testing program and standards, 847–848
- evaluate test results, 849–850
- exercise tests, 849
tests
- guidelines for resilient software and systems, 803–805
- release management and, 889–890
- Threat, Vulnerability and Incident Management, Operations, 57
- threat actor, 987
- threat motive, 987
- threats. See also vulnerabilities defined, 986
- manage insider threats, 963
- monitoring software and systems, 795
- protecting information assets, 518–519
- TIP (targeted improvement profile) capability level ratings overlaid on, 93–94
- overview of, 91–92
- TIRs. See targeted improvement roadmaps (TIRs)
- TM. See Technology Management (TM)
tools, techniques, and methods
- Access Management, 164
- Asset Definition and Management, 138
- Communications, 200–201
- Compliance, 232–233
- Controls Management, 262–263
- Enterprise Focus, 331
- Environmental Control, 297–298
- External Dependencies Management, 371–372
- Financial Resource Management, 403–404
generic goals and practices, 949–950
- Identity Management, 465–466
- Incident Management and Control, 502–503
- Knowledge and Information Management, 540–541
- Measurement and Analysis, 570–571
- Monitoring, 598–599
- Organizational Process Definition, 621–623
- Organizational Process Focus, 646–647
- Organizational Training and Awareness, 677–678
- People Management, 707–709
- Resilience Requirements Development, 760
- Resilience Requirements Management, 782
- Resilient Technical Solution Engineering, 817–818
- Risk Management, 737
- Service Continuity, 857
- Technology Management, 903
- Vulnerability Analysis and Resolution, 932
- traceability, of resilience requirements, 776–777
- tracking
- events in incident management, 480–481
- resilience requirements, 777
- training people
- Access Management, 167
- Asset Definition and Management, 138, 140
- Communications, 200–201
- Compliance, 232–233
- Controls Management, 262–263
- Enterprise Focus, 331
- Environmental Control, 297–298
- External Dependencies Management, 371–372
- Financial Resource Management, 403–404
- generic goals and practices, 949–950
- Identity Management, 465–466
- Incident Management and Control, 502–503
- Knowledge and Information Management, 540–541
- Measurement and Analysis, 570–571
- Monitoring, 598–599
- Organizational Process Definition, 621–623
- Organizational Process Focus, 646–647
- Organizational Training and Awareness, 677–678
- People Management, 707–709
- Resilience Requirements Development, 760
- Resilience Requirements Management, 782
- Resilient Technical Solution Engineering, 817–818
- Risk Management, 737
- Service Continuity, 857
- Technology Management, 903–906
- Vulnerability Analysis and Resolution, 934
training programs. See also Organizational Training and Awareness (OTA)
assess effectiveness of, 670–671
conduct, 668
deliver resilience training, 668–669
establish capability for, 666–668
establish needs, 664–665
establish plan, 665–666
record, 669–670
triaging events, in incident management, 482–483
trusted access. See Identity Management (IM)
typical work products, process areas defined, 46–48
typographical and structural conventions, 51
typographical conventions, 49–51
U
unplanned downtime, 890, 987
updating
measurement and analysis objectives, 559
process definitions and development plans, 810
service continuity plans, 846
vulnerability repository, 925
user IDs, access control via, 525
users, 987
utility sector, CERT-RMM in
about the authors, 99–100
grid modernization and transformation, 103–104
regulation and peer pressure, 101–103
reliability and resilience in, 100–101
V
validation
of compliance data, 221
of resilience requirements, 756
of service continuity plans, 845–846
validity and reliability of information assets, 529–530
VAR. See Vulnerability Analysis and Resolution (VAR)
verification
evaluating suitability of candidate staff, 418–420
managing access to assets during position changes, 430–431
version control, manage work product configurations and, 950
vital records
defined, 987
protecting, 513
vital staff. See also staff, 987
vital termination, of employment, 427
vulnerabilities
analysis and resolution strategy for, 918–920
analyze, 923–925
defined, 987
discover, 921–923
establish scope of, 917–918
identify root causes, 927–928
identify sources of, 920–921
manage exposure to, 925–927
monitoring software and systems for, 795
overview of, 915–916
protecting information assets, 518–519
service continuity planning and, 832
Vulnerability Analysis and Resolution (VAR)
achieve specific goals, 928
analyze vulnerabilities, 923–925
assign responsibility for, 933
collect improvement information, 940–941
defined, 987
discover vulnerabilities, 921–923
establish analysis and resolution strategy, 918–920
establish defined process, 940
establish process governance, 929–930
establish scope of assets and environments to be analyzed, 917–918
FISMA compliance, 961
identify and involve relevant stakeholders, 935–936
identify root causes, 927–928
identify sources of vulnerabilities, 920–921
insider threats and, 964
introductory notes, 915–916
manage exposure to vulnerabilities, 925–927
manage work product configurations, 935
monitor and control the process, 937–939
monitoring needs of, 586
objectively evaluate adherence, 939
plan the process, 930–931
prepare for vulnerability analysis and resolution, 917
provide resources for, 931–932
purpose of, 915
related process areas, 916
relationships driving threat/incident management, 57–58
review status with higher-level managers, 940
summary of specific goals and practices, 916
train people for, 934
vulnerability catalogs, 921
vulnerability data collection, 921
vulnerability management strategy, 987
vulnerability notification services, 921
vulnerability repository, 987
vulnerability resolution, 987
W
waivers, 987
White, David W., 999, xxiv
work environment standards, 614–615
work product configurations
Access Management, 168
Asset Definition and Management, 141
Communications, 202
Compliance, 234
Controls Management, 264
Enterprise Focus, 332
Environmental Control, 298–299
External Dependencies Management, 373
generic goals and practices, 950
Human Resource Management, 440–441
Identity Management, 466–467
Incident Management and Control, 504
Knowledge and Information Management, 541
Measurement and Analysis, 571
Monitoring, 599–600
Organizational Process Definition, 623
Organizational Process Focus, 647–648
Organizational Training and Awareness, 678–679
People Management, 709
Resilience Requirements Development, 763
Resilience Requirements Management, 785–786
Resilient Technical Solution Engineering, 821–822
Risk Management, 740
Service Continuity, 860
Technology Management, 906–907
Vulnerability Analysis and Resolution, 935
work products, typical
defined, 46–48
typographical and structural conventions, 51