CERT®-RMM, VERSION 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

SEI SERIES • A CERT® BOOK

Richard A. Caralli

Julia H. Allen

David W. White

Software Engineering Institute | Carnegie Mellon

The SEI Series in Software Engineering

Library of Congress Cataloging-in-Publication Data

Caralli, Richard A.
The CERT resilience management model : a maturity model for managing operational resilience / Richard A. Caralli, Julia H. Allen, David W. White.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-321-71243-1 (hardcover : alk. paper)
1. Organizational change. 2. Organizational effectiveness. 3. Crisis management. 4. Success in business. 5. Resilience (Personality trait) I. Allen, Julia H. II. White, David W. (David Warren), 1964- III. Carnegie-Mellon University. CERT Coordination Center. IV. Title.
HD58.8.C344 2011
658.4'7—dc22

2010037204

ISBN-13: 978-0-321-71243-1
ISBN-10: 0-321-71243-9

Text printed in the United States on recycled paper at Edwards Brothers in Ann Arbor, Michigan.
First printing, December 2010

CONTENTS

This page intentionally left blank

PREFACE

> Resilience (*noun*): the physical property of a material by which it can return to its original shape or position after deformation that does not exceed its elastic limit[1]

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

1. See http://wordnet.princeton.edu.

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.

CHAPTER 1

INTRODUCTION

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

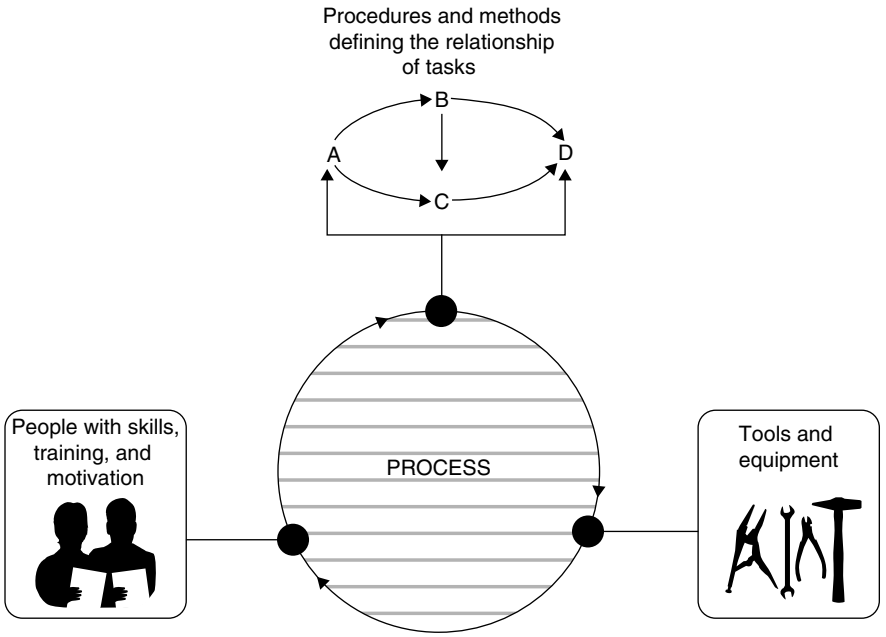

FIGURE 1.1
The Three Critical Dimensions

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

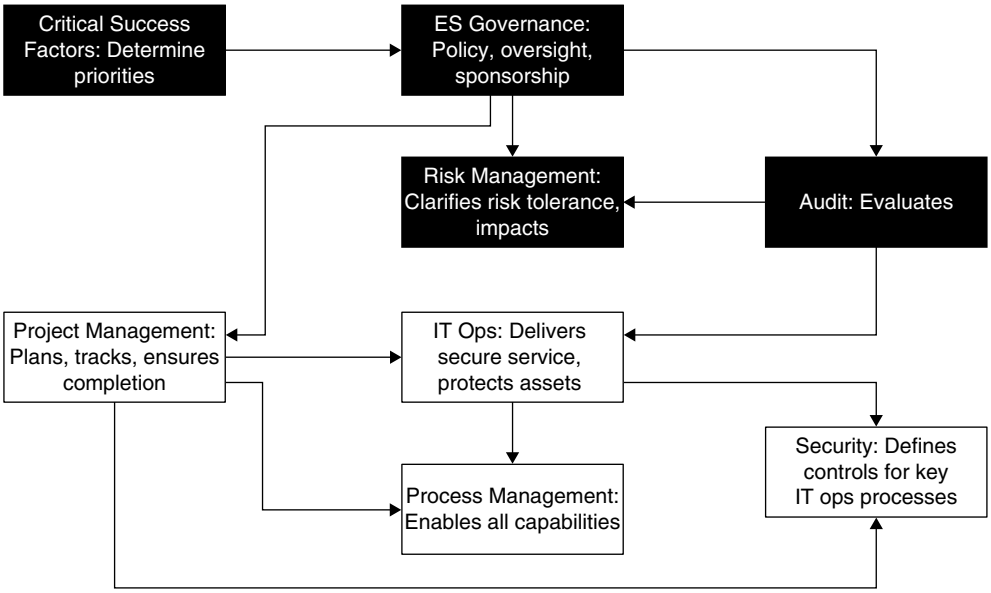

FIGURE 1.2
Bodies of Knowledge Related to Security Process Improvement

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,

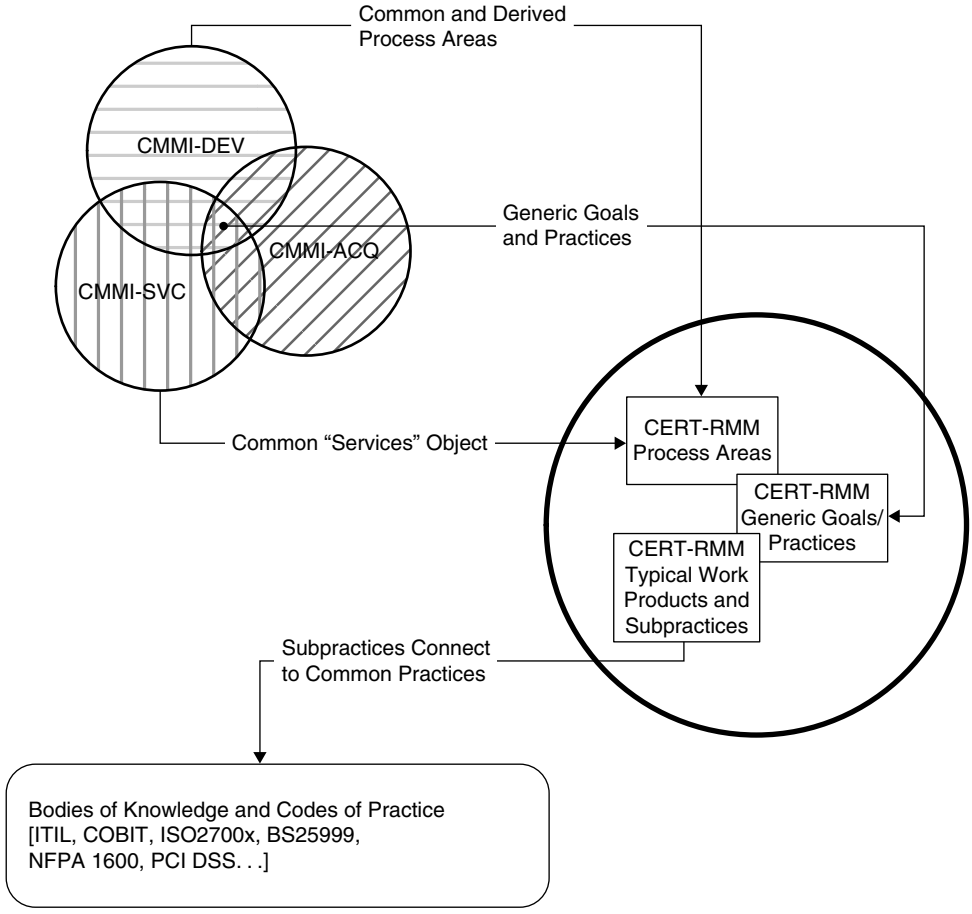

FIGURE 1.3
CERT-RMM Influences

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 1.1 Process Areas in CERT-RMM and CMMI Models

CMMI Models Process Areas	*Equivalent CERT-RMM Process Areas*
CAM—Capacity and Availability Management *(CMMI-SVC only)*	**TM—Technology Management** CERT-RMM addresses capacity management from the perspective of technology assets. It does not address the capacity of services. Availability management is a central theme of CERT-RMM, significantly expanded from CMMI-SVC. Service availability is addressed in CERT-RMM by managing the availability requirement for people, information, technology, and facilities. Thus, the process areas that drive availability management include • **RRD—Resilience Requirements Development** (where availability requirements are established) • **RRM—Resilience Requirements Management** (where the life cycle of availability requirements is managed) • **EC—Environmental Control** (where the availability requirements for facilities are implemented and managed) • **KIM—Knowledge and Information Management** (where the availability requirements for information are implemented and managed) • **PM—People Management** (where the availability requirements for people are implemented and managed) • **TM—Technology Management** (where the availability requirements for software, systems, and other technology assets are implemented and managed)

CMMI Models Process Areas	*Equivalent CERT-RMM Process Areas*
IRP—Incident Resolution and Prevention *(CMMI-SVC only)*	**IMC—Incident Management and Control** In CERT-RMM, IMC expands IRP to address a broader incident management system and incident life cycle at the asset level. Workarounds in IRP are expanded in CERT-RMM to address incident response practices.
MA—Measurement and Analysis	**MA—Measurement and Analysis** is carried over intact from CMMI. In CERT-RMM, MA is directly connected to MON—Monitoring, which explicitly addresses data collection that can be used for MA activities.
OPD—Organizational Process Definition	**OPD—Organizational Process Definition** is carried over from CMMI, but development-life-cycle–related activities and examples are deemphasized or eliminated.
OPF—Organizational Process Focus	**OPF—Organizational Process Focus** is carried over intact from CMMI.
OT—Organizational Training	**OTA—Organizational Training and Awareness** OT is expanded to include awareness activities in OTA.
REQM—Requirements Management	**RRM—Resilience Requirements Management** Basic elements of REQM are included in RRM, but the focus is on managing the resilience requirements for assets and services, regardless of where they are in their development cycle.
RD—Requirements Development	**RRD—Resilience Requirements Development** Basic elements of RD are included in RRM, but practices differ substantially.
RSKM—Risk Management	**RISK—Risk Management** 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.
SAM—Supplier Agreement Management	**EXD—External Dependencies Management** In CERT-RMM, SAM is expanded to address all external dependencies, not only suppliers. EXD practices differ substantially.
SCON—Service Continuity *(CMMI-SVC only)*	**SC—Service Continuity** In CERT-RMM, SC is positioned as an operational risk management activity that addresses what is required to sustain assets and services balanced with preventive controls and strategies (as defined in CTRL).
TS—Technical Solution	**RTSE—Resilient Technical Solution Engineering** RTSE uses TS as the basis for conveying the consideration of resilience attributes as part of the technical solution.

TABLE 1.2 Other Connections Between CERT-RMM and the CMMI Models

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

1.4 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 application of process improvement tools and techniques and provide a foundational platform for better and more sophisticated measurement methodologies and techniques. The ultimate goal in CERT-RMM is to ensure that operational resilience processes produce intended results (such as improved ability to manage incidents or an accurate asset inventory), and as the processes are improved, so are the results and the benefits to the organization. Because CERT-RMM is a process-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 organizational maturity for managing operational resilience by defining a prescriptive path through the model (i.e., by providing an order by which process areas should be addressed) requires additional study and research, and all indications from early model use, benchmarking, and piloting are that a capability maturity model for operational resilience management founded on CERT-RMM is achievable in the future.

This page intentionally left blank

INDEX

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W