Software Engineering Institute

CERT® Resilience Management Model Capability Appraisal Method (CAM) Version 1.1

Resilient Enterprise Management Team

October 2011

TECHNICAL REPORT
CMU/SEI-2011-TR-020
ESC-TR-2011-020

CERT® Program

http://www.sei.cmu.edu

Carnegie Mellon

This material is based upon work funded and supported by the United States Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

Contracting Officer
ESC/CAA
20 Shilling Circle
Building 1305, 3rd Floor
Hanscom AFB, MA 01731-2125

Table of Contents

List of Figures

List of Tables

Abstract

The CERT® Resilience Management Model (CERT®-RMM), developed by the CERT® Program at Carnegie Mellon University's Software Engineering Institute (SEI), 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. In operational terms, resilience is an *emergent* property of an organization that can continue to carry out its mission after a disruption that does not exceed its operational limit.

The ability of an organization to assess its current level of capability using CERT-RMM as the reference model is essential for measuring the current competency of its operational practices, setting improvement targets, and establishing plans and actions to close any gaps.

The SEI has developed and maintained the Standard Capability Maturity Model® Integration (CMMI®) Appraisal Method for Process Improvement (SCAMPI℠) family of appraisal methods from the CMMI product suite. Consultations with the SEI's CMMI program manager indicated that it would be appropriate to extend the pedigree of the SCAMPI family of appraisal methodologies for the CERT-RMM Capability Appraisal Method (CAM) Version 1.1.

This report demonstrates that the SCAMPI Version 1.2 method can be adapted and applied to CERT-RMM V1.1 as the reference model for a process appraisal.

Introduction

The CERT® Resilience Management Model (CERT®-RMM), developed by the CERT Program at Carnegie Mellon University's Software Engineering Institute (SEI), 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. In operational terms, resilience is an *emergent* property of an organization that can continue to carry out its mission after a disruption that does not exceed its operational limit. Resilience 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" [Humphrey 1989] by defining *quality* as the extent to which an organization controls its ability to operate in a mission-driven, complex risk environment.

CERT-RMM Version 1.1 contains 26 process areas that cover four areas of operational resilience management: enterprise management, engineering, operations, and process management. The practices contained in these process areas are codified from a management perspective; that is, the practices focus on the activities that an organization performs to actively *direct*, *control*, and *manage* operational resilience in an environment of uncertainty, complexity, and risk. For example, the model does not prescribe specifically how an organization should secure information; instead, it focuses on the equally important processes of identifying high-value assets, making decisions about the capability levels needed to protect and sustain these assets, implementing strategies to achieve these capability levels, and maintaining these levels throughout the life cycle of the assets during stable times and, more importantly, during times of stress. 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.

The ability of an organization to assess its current level of capability using CERT-RMM as the reference model is essential for measuring the current competency of its operational practices, setting improvement targets, and establishing plans and actions to close any identified gaps.

The objectives for a CERT-RMM Capability Appraisal Method (CAM) require that the method

- be repeatable
- provide objective proof of the achievement of specific and generic goals and performance of specific practices in a process area
- support internally or externally led appraisals
- be suitable for deriving and supporting capability level ratings
- provide high-quality results that can be substantiated

The unique aspects of CERT-RMM—the process focus and the capability dimension—help organizations to better manage operational resilience and sustain capabilities over the long run. Regardless of the scope of improvement—a single aspect of operational resilience such as incident management or a broad, comprehensive scope that incorporates all 26 process areas—CERT-RMM enables an organization to easily begin a process improvement approach.

The SEI has invested a considerable amount of time and energy developing and maintaining the Standard Capability Maturity Model® Integration (CMMI®) Appraisal Method for Process Improvement (SCAMPI℠) family of appraisal methods from the CMMI product suite. The SCAMPI method has a proven track record and a large and knowledgeable community of users, and it is suitable for use with many reference models. Consultations with the SEI's CMMI program manager indicated that it would be appropriate to extend the pedigree of the SCAMPI family of appraisal methodologies for the CERT-RMM Capability Appraisal Method (CAM) Version 1.1. Using SCAMPI principles enables the development of a CERT-RMM appraisal method without extraordinary investment and provides a standard appraisal method for the entire SEI family of process improvement models.

This report demonstrates that the SCAMPI Version 1.2 method can be adapted and applied to CERT-RMM V1.1 as the reference model for a process appraisal [Caralli 2010]. The report was developed using material from *Standard CMMI Appraisal Method for Process Improvement (SCAMPI), Version 1.2: Method Definition Document SEI-2006-HB-002* [SCAMPI 2006] and *Interpreting SCAMPI for a People CMM Appraisal at Tata Consultancy Services* [Radice 2005].

Like SCAMPI, three classes of appraisal methods—A, B, and C—are envisioned for the CERT-RMM capability appraisals. The class A appraisal method is the most rigorous and is the focus of this report. Reports on class B and class C methods will follow.

Class A appraisals can be performed in three modes of usage as depicted in Table 1.

Table 1: Three Usage Modes of CERT-RMM Class A Appraisal

Usage Mode	Description
Internal Process Improvement	Organizations appraise internal processes to baseline their capability level(s), establish or update a process improvement program, or measure progress in implementing a process improvement program.
Supplier Selection	Appraisal results are used as a high-value discriminator to select third-party suppliers, vendors, or other external service providers. The ability of a key supplier to demonstrate operational resilience under times of stress may provide a competitive business advantage to an organization.
Process Monitoring	Appraisals may also be used to monitor processes, both internal and external to the organization, prioritize and tailor improvement efforts, track key risk indicators, and monitor the performance of external entities and suppliers.

It is important to keep all stakeholders focused on the fact that a CERT-RMM class A capability appraisal is intended as a benchmarking appraisal method suitable for generating capability level ratings. As a benchmarking method, the emphasis of CERT-RMM CAM V1.1 is on a rigorous method capable of achieving high accuracy and reliability of appraisal results through the collection of objective evidence from multiple sources. This method is not well suited for organizations that have a limited understanding of model-based process improvement or of CERT-RMM. Such organizations may not yet have a clear idea of how the practices described in the reference model ought to be implemented to meet their specific business needs. A different type of appraisal (CAM class B or C) or assessment (CERT-RMM Compass) is probably more

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

℠ SCAMPI is a service mark of Carnegie Mellon University.

valuable if the objective of the sponsor is to begin the process of understanding what model-based process improvement could mean for the organization.

CERT-RMM Compass is a lightweight assessment instrument that can provide organizations with a quick "health check." By identifying areas of concern, CERT-RMM Compass helps to prioritize and set the direction for more formal improvement efforts. CERT-RMM Compass takes the content of CERT-RMM and forms it into questions that elicit insight into practices performed, incomplete practices, and institutionalizing factors (such as governance, training, policy, and measurement) that support the retention of practices under stressful conditions. CERT-RMM Compass questions are scored based on organizational responses, and scores are interpreted in several dimensions.

CERT-RMM Navigator is an assessment certification role. The Navigator prepares individuals to administer and score CERT-RMM Compass. The Navigator facilitates the collection of information and self-assessment using the CERT-RMM Compass instrument and participates in the scoring activity. The Navigator then facilitates a discussion of the CERT-RMM Compass results and catalyzes the improvement planning activity. Having certified Navigators among an organization's personnel provides the flexibility to extend improvement efforts throughout the organization.

There are many effective and appropriate ways for an organization to use CERT-RMM to guide, inform, or otherwise support improvements to its operational resilience management activities. For those familiar with process improvement, CERT-RMM can be used as the body of knowledge that supports model-based process improvement activities for operational resilience management processes. However, not all organizations embrace process improvement and are simply looking for a way to evaluate their operational performance or organize their practices. CERT-RMM Compass may be an appropriate starting point for organizations that are just getting acquainted with this body of work or that have a need to address a specific problem area such as incident management or insider threat. All of these uses of CERT-RMM are legitimate.

To ensure simplicity and save effort, the SCAMPI Method Definition Document V1.2 (MDD) is used as the primary basis for the CERT-RMM V1.1 CAM.

Traceability is maintained with SCAMPI MDD V1.2 by using the same numbering sequence for the processes outlined in CERT-RMM CAM V1.1. Minor edits to clarify terminology and language will not affect usability of the CERT-RMM CAM report. The traceability matrix may be found in Appendix A.

The Glossary provides further explanation of terms that CERT-RMM uses differently.

The following sections in this report present the process definitions used to perform a capability appraisal of CERT-RMM V1.1 process areas based on SCAMPI MDD V1.2, with interpretations and terminology changes as noted in the Glossary.

Purpose

An objective, repeatable, and transitionable appraisal method is needed to support the adoption and use of CERT-RMM by its intended community.

This report provides information to enable security practitioners, business continuity specialists, and current lead appraisers (and trainees) to accurately interpret the evidentiary artifacts when using CERT-RMM as the reference model.

Background

Currently, operational risk management practitioners, particularly when managing business continuity, information security, and IT operations, must rely on best-practice-based approaches to determine their capability for managing operational risk and resilience. Assessment instruments are typically self-scoring questionnaires or checklist-driven reviews based on commonly used codes of practice such as the ISO27000 series, NIST special publications, ITIL, BS25999, or COBIT. These point-in-time reviews using codes of practice as a benchmark have some limitations:

- They are limited in scope to the area of operational risk that is the subject of the code of practice (e.g., ISO27002 reviews concentrate primarily on information security).
- They establish that the organization is performing the practices only at the time of the review.
- They do not evaluate how the organization will perform under times of stress or whether they will be able to sustain and repeat their successes in the long run. In other words, there is no evaluation of the organization's ability to sustain operational processes.

Currently, evaluation of the practices in the domains composing operational resilience (information security, business continuity, and IT operations) significantly lags behind evaluation of the practices in the software and systems engineering domain for two primary reasons:

- Codes of practice in the operational resilience domain typically do not have a process orientation, thus preventing the application of process maturity concepts.
- Codes of practice that claim to include a maturity representation incorrectly apply process maturity concepts typically resulting in a useful but not necessarily effective structure for categorizing practices and defining a progression or sequence of practices to implement.

CERT-RMM provides the community with the first usable process definition for managing operational resilience that correctly applies the concepts of process institutionalization and capability maturity. This enables effective capability appraisals and supports a true process improvement approach to managing operational resilience. To accomplish this, CERT-RMM leverages the SEI's process maturity expertise in developing and transitioning CMMI to define a capability-based, continuous representation that can be used to characterize process implementation in an organization.

Capability Levels

CERT-RMM currently defines four capability levels, designated by the numbers 0 through 3, as follows in Table 2:

Table 2: Capability Levels in CERT-RMM

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

In the CERT-RMM appraisal reference model, there is a direct relationship between goals (specific and generic) and practices (specific and generic) that contribute to the achievement of those goals. Specific and generic goals are required model components; specific and generic practices are expected model components.

A fundamental premise in the CERT-RMM CAM V1.1 method is that satisfaction of goals can be determined only upon detailed investigation of the extent to which each corresponding practice is implemented for each practice instantiation used as the basis for the appraisal.

A capability level for a process area is achieved when all of the generic goals are satisfied up to that level. By design, Capability Level 2 is defined by Generic Goal 2, and Capability Level 3 is defined by Generic Goal 3. Thus, the generic goals and practices at each level define the meaning of the capability levels. Because capability is cumulative, reaching Capability Level 3 means that the organization is also performing the goals and practices at Capability Levels 1 and 2. When establishing capability level targets, the organization should consider the importance of the generic practices relative to the organization's risk tolerance, threat environment, size, improvement time frame, and improvement objectives. It may be valuable to review the generic goals and generic practices and envision what the implementation of those practices and the achievement of those goals would look like for the organization during normal operations and in times of stress. Capability level targets should be established for each process area that is to be appraised and need not be the same. Capability Level 1 (performed) may be completely appropriate for one process area, even if Capability Level 3 (defined) is the established target for another process area in the model scope.

Tailoring SCAMPI for Use with CERT-RMM

CMMI V1.2 includes three integrated models: CMMI for Development (CMMI-DEV), CMMI for Acquisition (CMMI-ACQ), and CMMI for Services (CMMI-SVC). The CMMI Framework provides a common structure for CMMI models, training, and appraisal components. The primary difference between using the appraisal processes with the CMMI-DEV and CMMI-ACQ reference models and the CERT-RMM reference model is the point at which the practices occur in the life cycle of the organization. As Figure 1 shows, the CMMI-DEV and CMMI-ACQ are focused on the early systems development life cycle, which includes planning, designing, acquiring, developing, and deploying. CERT-RMM is focused on the operations life cycle of the organization, which includes primarily the deployment, day-to-day operations, and decommissioning of information, technology, people, and facility assets. CERT-RMM also addresses resilience requirements development in the early life cycle of all assets.

The CMMI-SVC model shares the core process areas of the CMMI-DEV and CMMI-ACQ models but also includes operational aspects of service delivery. Both CMMI-SVC and CERT-

RMM promote a requirements-driven, engineering-based approach to developing and implementing resilience strategies for assets in the operational environment.

Appraisals using SCAMPI with the CMMI-DEV, CMMI-ACQ, and CMMI-SVC as the reference models have traditionally been used and facilitated by systems and software developers, although with the release of the CMMI-SVC model, the community of interested users has expanded. The initial practitioners most likely to use and facilitate CERT-RMM appraisals will include current SCAMPI lead appraisers (LAs), business continuity professionals, information or physical security practitioners, and information technology operators.

This report is not intended to provide a solid foundation in the SCAMPI method but rather a description of how SCAMPI processes are adapted, interpreted, and used in CERT-RMM appraisals.

Community input will be important for evolving our knowledge of the appraisal process to an operational environment.

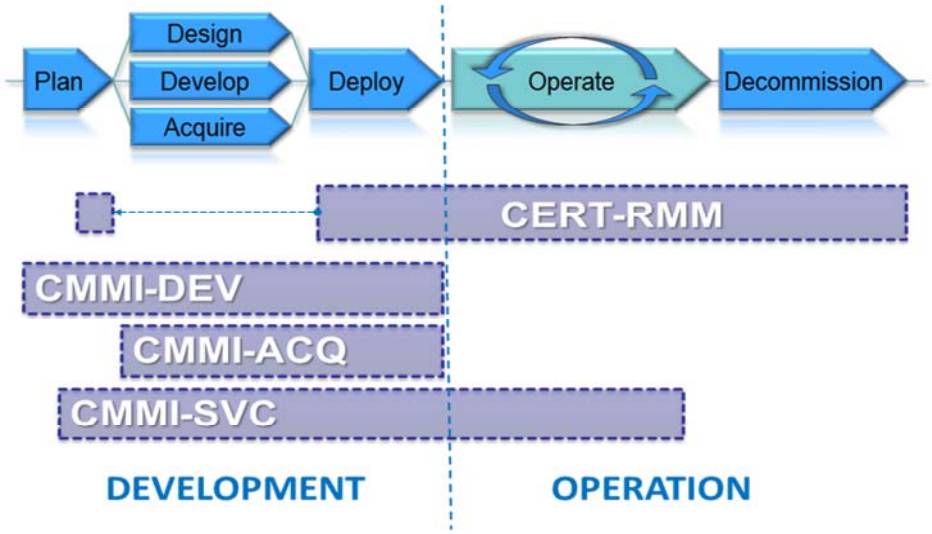

Figure 1: The CMMI-DEV, CMMI-ACQ, CMMI-SVC, and CERT-RMM Positions in the Organizational Life Cycle

The SCAMPI MDD is the formal definition of the class A appraisal method. This report is modeled on the SCAMPI Class A MDD V1.2 and attempts to highlight the differences between the SCAMPI class A method and the CERT-RMM class A Capability Appraisal Method (CAM). The guidance provided in this report is supplemental to the SCAMPI MDD V1.2; it is not a replacement guide. This report describes how the SCAMPI processes are used in a CERT-RMM class A capability appraisal.

SCAMPI is a family of appraisal methods that is part of the CMMI Product Suite. SCAMPI can be used in the class C mode as an assessment instrument and in the class A mode as a capability evaluation, which results in a capability level rating. Considerable resources have been expended to develop and maintain SCAMPI as an objective and reliable appraisal method. In practice, SCAMPI is described as follows [SCAMPI 2006]:

The SCAMPI appraisal methods are the generally accepted methods used for conducting appraisals using CMMI models. The SCAMPI Method Definition Document (MDD) defines rules for ensuring the consistency of appraisal ratings. For benchmarking against other organizations, appraisals must ensure consistent ratings. The achievement of a specific maturity level or the satisfaction of a process area must mean the same thing for different appraised organizations.

The SCAMPI family of appraisals includes Class A, B, and C appraisal methods. SCAMPI A is the most rigorous method and the only method that can result in a rating. SCAMPI B provides options in model scope, but the characterization of practices is fixed to one scale and is performed on implemented practices. SCAMPI C provides a wide range of options, including characterization of planned approaches to process implementation according to a scale defined by the user.

The SCAMPI methods are backed at the SEI by rigorous training and authorization processes, data collection procedures and systems, and quality control processes. All of this is designed to make SCAMPI repeatable and reliable as a benchmarking tool.

A significant conceptual difference between the CERT-RMM appraisal method and the SCAMPI appraisal method arises from the difference in focus between CMMI-DEV and CERT-RMM. The objective of CMMI-DEV is to transform the quality of the work output of software and systems development projects by maturing development processes in the organization. Therefore, for CMMI-DEV, the nominal focal point in the organization is a project, and SCAMPI is designed to evaluate practices at the project level to determine whether the goals of CMMI-DEV are being achieved.

Operational resilience for an organization cannot be determined at the project level. Therefore, for CERT-RMM appraisals, the nominal focal point is larger than a project: it is a unit of the organization. An organizational unit (OU) is a single, distinct, well-defined organizational component (e.g., department, line of business, business unit, or program) of an organization. Typically, such a unit is at a sufficient level in the organizational structure that the unit has responsibility for processes that contribute to the organization's operational resilience (via capable processes and practices). In some cases and for some process areas, the nominal unit for the CERT-RMM's focus in an organization will be defined as the entire enterprise. In CERT-RMM, there is no project focus. As a result, the CERT-RMM CAM evaluates practices in an organization at the level of a defined organizational unit, which is typically a higher-level component than a project. As a result, rules for sufficient coverage, organizational scope, model scope, and evidence must be defined for CERT-RMM in a way that is distinct from those concepts in CMMI-DEV. The CMMI-SVC team has addressed some of these issues because CMMI-SVC is similar to CERT-RMM in this respect.

The focus of CERT-RMM is broader than the focus of CMMI-DEV. CERT-RMM covers the processes required to establish, deliver, and manage operational resilience activities in order to ensure continued performance of organizational assets and services in support of the mission. 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. 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 defined as people, information, technology, and facilities. However, the use of CERT-RMM in a production environment is not precluded; 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.

The CERT-RMM CAM is composed of three phases (see Table 3, Table 4, and Table 5), each of which has one or more processes. These are further described in the subsequent sections of this report.

Table 3: CERT-RMM CAM Phase 1: Plan and Prepare for Appraisal

Phase	Process	Purpose	CERT-RMM CAM V1.1 Activities
1. Plan and Prepare for Appraisal	1.1 Analyze Requirements	To understand the organization's business objectives for the appraisal. The appraisal team leader will assist the appraisal sponsor in matching the business objectives with the appraisal objectives.	1.1.1 Determine Appraisal Objectives 1.1.2 Determine Appraisal Constraints 1.1.3 Determine Appraisal Scope 1.1.4 Determine Outputs 1.1.5 Obtain Commitments to Appraisal Input
	1.2 Develop Appraisal Plan	To document requirements, agreements, risks, estimates, method tailoring, and other considerations (e.g., schedules, logistics, resources, contextual information about the organization) for the appraisal. Obtain, record, and make visible the sponsor's approval of the appraisal plan.	1.2.1 Tailor Method 1.2.2 Identify Needed Resources 1.2.3 Determine Cost and Schedule 1.2.4 Plan and Manage Logistics 1.2.5 Document and Manage Risks 1.2.6 Obtain Commitment to Appraisal Plan
	1.3 Select and Prepare Team	To ensure that an experienced, trained, appropriately qualified team is available and prepared to execute the appraisal plan.	1.3.1 Identify Appraisal Team Leader 1.3.2 Select Team Members 1.3.3 Prepare Team
	1.4 Obtain and Inventory Initial Objective Evidence	To obtain data on model practices in place and identify potential issues, gaps, or risks to aid in refining the appraisal plan. Obtain a preliminary understanding of the organization's structure, operations, and processes.	1.4.1 Obtain Initial Objective Evidence 1.4.2 Inventory Objective Evidence
	1.5 Prepare for Appraisal Conduct	To plan and document specific data collection strategies, including sources of data, tools, methods, and technologies used. Prepare contingencies to manage the risk of insufficient data.	1.5.1 Perform Readiness Review 1.5.2 Prepare Data Collection Plan 1.5.3 Replan Data Collection (if needed)

Table 4: CERT-RMM CAM Phase 2: Conduct Appraisal

Phase	Process	Purpose	CERT-RMM CAM V1.1 Activities
2. Conduct Appraisal	2.1 Prepare Participants	To ensure the organization's appraisal participants understand the purpose of the appraisal and are prepared to participate.	2.1.1 Conduct Participant Briefing
	2.2 Examine Objective Evidence	To collect information about the practices implemented in the organization and relate the resultant data to the appraisal reference model and organizational scope.	2.2.1 Examine Objective Evidence
	2.3 Document Objective Evidence	To create lasting records of the information gathered by the appraisal team.	2.3.1 Take/Review/Tag Notes 2.3.2 Record Presence/Absence of Objective Evidence 2.3.3 Document Practice Implementation 2.3.4 Review and Update the Data Collection Plan
	2.4 Verify Objective Evidence	To verify the implementation of the organization's practices for the appraisal reference model and organizational scope.	2.4.1 Verify Objective Evidence 2.4.2 Characterize Implementation of Model Practices
	2.5 Validate Preliminary Findings	To validate the preliminary findings with the appraisal participants. This process is the final data collection opportunity.	2.5.1 Validate Preliminary Findings
	2.6 Generate Appraisal Results	To rate the satisfaction of the goals, based on the extent of practice implementation, for the appraisal reference model and organizational scope.	2.6.1 Derive Findings and Rate Goals 2.6.2 Determine Process Area Capability Level 2.6.3 Determine Capability Profile 2.6.4 Document Appraisal Results

Table 5: CERT-RMM CAM Phase 3: Report Results

Phase	Process	Purpose	CERT-RMM CAM V1.1 Activities
3. Report Results	3.1 Deliver Appraisal Results	To provide credible appraisal results that can be used to guide decision making in the organization.	3.1.1 Deliver Final Findings 3.1.2 Conduct Executive Session(s) 3.1.3 Plan for Next Steps
	3.2 Package and Archive Appraisal Assets	To preserve important data and records from the appraisal and dispose of sensitive materials in an appropriate manner.	3.2.1 Collect Lessons Learned 3.2.2 Generate Appraisal Record 3.2.3 Provide Appraisal Feedback to CERT-RMM Steward 3.2.4 Archive and/or Dispose of Key Artifacts

How to Use This Report

This report is primarily based on SCAMPI MDD V1.2 and experience gained from using CERT-RMM in appraisals with some minor input from SCAMPI MDD V1.3. Basic guidance and required practices for performing a CERT-RMM class A capability appraisal are provided here for ease of use. For additional explanations, tailoring guidance, or more specific implementation examples, consult SCAMPI MDD V1.2.

To maintain consistency and fidelity with SCAMPI MDD V1.2, the numbering scheme, names of processes, and activities used for each of the CERT-RMM CAM processes are the same as in SCAMPI MDD V1.2. However, because CERT-RMM has only a continuous representation, certain activities present in SCAMPI MDD V1.2 have been eliminated or modified significantly in this report. A table is provided in Appendix A to maintain traceability between the SCAMPI MDD V1.2 phases and processes and the CERT-RMM CAM phases and processes.

To provide an appraisal method that applies to a wide a range of situations and allows for flexibility and tailoring, some of the practices are intentionally stated without many implementation details. The practice descriptions use phrases like “adequate,” “sufficient,” “as appropriate,” and “as needed.” The use of such nonspecific terms allows for the widest possible interpretation and application of the practices. In many cases, definitions or examples are provided for nonspecific terms upon their first use. These phrases may have different meanings for two different organizations, for two units in a single organization, or for one unit at different points in its operational cycle. Each organizational unit must interpret these nonspecific phrases for its own situation. These nonspecific phrases are used so that goals and practices can be interpreted in light of an organization’s business objectives.

CERT-RMM uses phrases and/or terms that may not be found in other Capability-Maturity-Model (CMM)-based models or appraisal methods. In other cases the definition or use of these phrases and terms in CERT-RMM may be different from the definition or use as found in other CMM-based models. This report uses CERT-RMM phrases and terms and provides assistance with the definition and use of these in the context of a CERT-RMM appraisal.

The term “project(s)” from the CMMI models should be interpreted as organizational unit(s), superunit(s), or subunit(s) in CERT-RMM. Refer to the CERT-RMM glossary [Caralli 2010] for the definitions of organizational unit, superunit, and subunit. Therefore, when using SCAMPI MDD V1.2 as a reference document, the term “sample projects” should be interpreted as “sample organizational units and/or superunits or subunits.”

CERT-RMM has only a continuous representation, so any references to the staged representation that appears in SCAMPI MDD V1.2 are not used in this report because they are not relevant for CERT-RMM. Therefore, any reference to “model representation” means “continuous.” The term “capability level” to denote process-level capability is applicable for CERT-RMM. The term “maturity level” is not applicable other than implicitly, to infer that an organization with higher levels of process capability in one or more CERT-RMM process areas is likely more mature in its execution of process area practices.

1 Plan and Prepare for the Appraisal

Planning and preparing for the appraisal (Table 6) has five processes: Analyze Requirements, Develop Appraisal Plan, Select and Prepare Team, Obtain Initial Objective Evidence, and Prepare for Appraisal Conduct. Each process has tasks and activities explained in subsequent sections.

The CERT-RMM appraisal sponsor's objectives for appraisal are generally determined in the first process of the first phase (Phase 1 Plan and Prepare for Appraisal, Activity 1.1.1, Determine Appraisal Objectives). All other planning, preparation, execution, and reporting of results proceed from this initial activity according to the processes outlined in CERT-RMM CAM V1.1.

To be consistent with SCAMPI for CMMI, the appraisal scope for CERT-RMM comprises the model scope and the organizational scope. Organizational scope comprises the appropriate organizational units, superunits, and subunits as defined in the Appraisal Disclosure Statement (ADS). [1] All organizational units within an organization are assumed to share a common top-level manager and common policies. The Appraisal Disclosure Statement should reflect any differences in each individual appraisal.

Organizational units are selected as entities for appraisal based upon the defined CERT-RMM model scope and the sponsor's appraisal objectives. The primary functional domains in the CERT-RMM model are security, business continuity, and IT operations. This may make the selection of organizational entities in the appraisal scope less arbitrary than in a traditional appraisal using SCAMPI for CMMI. Thus it is important to ensure adequate evidence collection, verification, and validation of the practices selected in the model scope.

[1] An Appraisal Disclosure Statement (ADS) is a summary statement describing the ratings generated as outputs of the appraisal and the conditions and constraints under which the appraisal was performed. The ADS should be used for public disclosures of capability level ratings so they can be interpreted accurately.

Table 6: Plan and Prepare for the Appraisal

Process	Activity
1.1 Analyze Requirements	1.1.1 Determine Appraisal Objectives
	1.1.2 Determine Appraisal Constraints
	1.1.3 Determine Appraisal Scope
	1.1.4 Determine Outputs
	1.1.5 Obtain Commitment to Appraisal Input
1.2 Develop Appraisal Plan	1.2.1 Tailor Method
	1.2.2 Identify Needed Resources
	1.2.3 Determine Cost and Schedule
	1.2.4 Plan and Manage Logistics
	1.2.5 Document and Manage Appraisal Risks
	1.2.6 Obtain Commitment to Appraisal Plan
1.3 Select and Prepare Team	1.3.1 Identify Appraisal Team Leader
	1.3.2 Select Team Members
	1.3.3 Prepare Team
1.4 Obtain Initial Objective Evidence	1.4.1 Obtain Initial Objective Evidence
	1.4.2 Inventory Objective Evidence
1.5 Prepare for Appraisal Conduct	1.5.1 Perform Readiness Review
	1.5.2 Prepare Data Collection Plan
	1.5.3 Replan Data Collection

1.1 Analyze Requirements

At this early stage in the process, gathering information that supports good planning is most important. Often, the appraisal team leader must educate members of the sponsor's organization about the purpose and role of appraisals. Collaborative consultation between the appraisal team leader and the appraisal sponsor is important in this activity. The appraisal team leader may simply be able to interview the sponsor to get the needed information and reach agreements. In some settings, a series of meetings with different stakeholders may be needed to elicit and build consensus on the business needs that can be met through a CERT-RMM capability appraisal.

Understanding the history of appraisals in the organization, especially the organizational and appraisal reference model scope of past appraisals, is important for understanding the requirements for the appraisal under consideration. The choices sponsors make about appraisal scope are often tied to their (sometimes unstated) priorities for process improvement. Appraisals should not be isolated from other activities relating to process management and improvement.

Analysis of requirements is a foundation for the success of the entire appraisal; it is at this point in the appraisal that the most leverage exists for avoiding problems and issues downstream. Gathering and understanding the requirements for the conduct of a CERT-RMM class A capability appraisal is vital to making appropriate decisions and providing value to the sponsor. Many examples of problems encountered during appraisals can be traced to shortcomings in the conduct of this process.

The objectives that motivate the conduct of an appraisal must be well understood so that appropriate participants, tailoring decisions, and appraisal outputs can be selected. The constraints

that shape the conduct of the appraisal may limit the achievement of appraisal objectives and desired results if they are not adequately understood and negotiated. A clear agreement regarding appraisal outputs and their intended use helps sustain the sponsorship needed for conducting the appraisal and acting on the results. Establishing agreement on these objectives, constraints, outputs, and intended use forms the basis for sponsor and stakeholder commitment to the appraisal plan.

This process is composed of five activities, summarized in Table 7 and described below.

Table 7: Analyze Requirements

Process/Activity	Required Practices
1.1 Analyze Requirements	
1.1.1 Determine Appraisal Objectives	The appraisal team leader or designee shall • identify sponsor and relevant stakeholders and establish communication • document the business objectives provided by the sponsor and the specific appraisal objectives • ensure the alignment of the appraisal objectives to the business objectives • determine and document the appraisal usage mode (i.e., internal process improvement, supplier selection, or process monitoring)
1.1.2 Determine Appraisal Constraints	The appraisal team leader or designee shall • establish high-level cost and schedule constraints • determine which process areas (PAs) and organizational units are to be included • determine minimum, maximum, or specific sample size or coverage that is desired for the appraisal • negotiate constraints and objectives with stakeholders to ensure feasibility • document negotiated constraints to be met
1.1.3 Determine Appraisal Scope	The appraisal team leader, in conjunction with the appraisal sponsor and/or the sponsor's designee, shall • determine and document the reference model scope and representation to be used for the appraisal (CERT-RMM has continuous representation only) • determine and document the organizational units to be appraised • determine and document the organizational scope of the appraisal • identify and document the names of individuals who will participate in the appraisal
1.1.4 Determine Outputs	The appraisal team leader or designee shall • review required CERT-RMM class A capability appraisal outputs with the appraisal sponsor • review and select optional CERT-RMM class A capability appraisal outputs with the appraisal sponsor • determine the recipients of appraisal outputs based on sponsor instructions
1.1.5 Obtain Commitment to Appraisal Input	The appraisal team leader or designee shall • record required information in the appraisal input • obtain sponsor approval of the appraisal input • manage changes to the appraisal input, obtaining sponsor approval of changes

1.1.1 Determine Appraisal Objectives

The business needs for process improvement drive the requirements for the conduct of any given appraisal and generally include one or more closely related factors:

- reducing cost of controls and compliance
- improving the organization's ability to protect and sustain high-value services and their associated assets, particularly during times of stress and disruption

The fundamental premise of process improvement is that organizational processes significantly impact these factors. Obtaining a fair and objective characterization of the processes in use in the organization is the essential reason for conducting an appraisal. In addition to this motivation, a sponsor's desire to conduct an appraisal could be driven by one or more of the following business-related objectives:

- Document a credible benchmark that serves as a baseline against which process improvement investments and actions can be measured.
- Evaluate areas of operational risk that may affect the performance of the organization.
- Involve members of the appraised organization in improving the performance of their operational resilience processes.
- Inform specific decisions related to the direction of a new or existing improvement program.
- Evaluate external dependencies (suppliers) that potentially affect operational resilience.

Organizations with experience in the use of appraisals may have identified a clear set of appraisal objectives in advance of designating an appraisal team leader.

In some cases, the usage mode is self-evident; however, there may be instances in which the appraisal sponsor either may not be sure about the usage mode or may have made an assumption that is not founded on fact. The appraisal team leader is responsible for ensuring that the choice of usage mode is consistent with the sponsor's input and direction.

Table 8 summarizes this activity.

Table 8: Analyze Requirements: Determine Appraisal Objectives

Process/Activity	Required Practices
1.1 Analyze Requirements	
1.1.1 Determine Appraisal Objectives	The appraisal team leader or designee shall • identify sponsor and relevant stakeholders and establish communication • document the business objectives provided by the sponsor and the specific appraisal objectives • ensure the alignment of the appraisal objectives to the business objectives • determine and document the appraisal usage mode (i.e., internal process improvement, supplier selection, or process monitoring)

1.1.2 Determine Appraisal Constraints

The constraints within which the appraisal must be conducted are determined based on a dialogue between the appraisal team leader and the appraisal sponsor. This dialogue is typically an iterative process in which the preferences of the appraisal sponsor, the limits of the method, and the consequent resource requirements are balanced against each other to arrive at an optimal set of appraisal input parameters. Constraints on cost and schedule identified during this early stage of the appraisal are expected to be high-level, not detailed estimates. They may take the form of statements such as "We need this done in Q4," "You can't use more than five of my people on the team," and "I can't afford to have the appraisal last more than two weeks."

Considerations for the appraisal data collection strategy may also be part of this activity. The data collection strategy outlines the overall high-level scheme for data collection, including the choice of a data collection approach, when the data will be collected, and what data collection techniques will be used. A well-defined data collection strategy is important for appraisal planning as it provides the basis for detailed data collection planning (see Activity 1.5, Prepare for Appraisal Conduct) and examining objective evidence (see Activity 2.2, Examine Objective Evidence).

Practical limitations relating to time, cost, and effort are clarified and negotiated in the context of other sponsor requirements. The business context in which the appraisal is conducted drives choices that the appraisal team leader must make. For example, if virtual methods (e.g., video conferences, teleconferences, and other similar technology) are to be used to conduct appraisal activities, the constraints imposed by these methods should be discussed, documented, and taken into account as the appraisal is planned.

Table 9 summarizes this activity.

Table 9: Analyze Requirements: Determine Appraisal Constraints

Process/Activity	Required Practices
1.1 Analyze Requirements	
1.1.2 Determine Appraisal Constraints	The appraisal team leader or designee shall • establish high-level cost and schedule constraints • determine which process areas (PAs) and organizational units are to be included • determine minimum, maximum, or specific sample size or coverage that is desired for the appraisal • negotiate constraints and objectives with stakeholders to ensure feasibility • document negotiated constraints to be met

1.1.3 Determine Appraisal Scope

The appraisal scope consists of the appraisal reference model scope and the organizational scope to be examined during the appraisal. The reference model scope must be determined and documented early in the planning process using the continuous representation of the CERT-RMM model. In conjunction with the appraisal sponsor, the appraisal team leader is responsible for making decisions regarding the process areas (PAs) included in the scope of the appraisal. The selection of appraisal outputs (see Section 1.1.4) should be driven by the understanding of their intended use and may dictate some selections when determining the reference model scope.

Organizational Scope

The organizational scope is defined as the part of an organization that is the subject of an appraisal and to which the appraisal results will be generalized. The organizational scope may include the entire organization or one or more units within the organization. For CERT-RMM appraisals, the nominal focal point is typically larger than a project (in SCAMPI MDD terms): it is a unit of the organization. An organizational unit is a single, distinct, well-defined organizational component (e.g., department, division, section, line of business, business unit, or program). Such a unit should be at a sufficient level in the organizational structure that the unit has responsibility for processes that contribute to the organization's operational resilience. In some cases and/or for some process areas, the organizational scope for the CERT-RMM appraisal is defined as the entire enterprise.

To clarify further, the following terms can be used to describe the organizational scope for the purposes of a CERT-RMM appraisal:

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

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

Figure 2 shows the typical relationship between organizational unit, organizational subunit, and organizational superunit on a generic organizational chart. In this example, the organizational unit is defined as a specific segment of the organization as shown on the organizational chart with multiple subunits. In this example, "organizational superunit" can refer to element 1 on the organization chart, as shown; it can also refer to the entire organization.

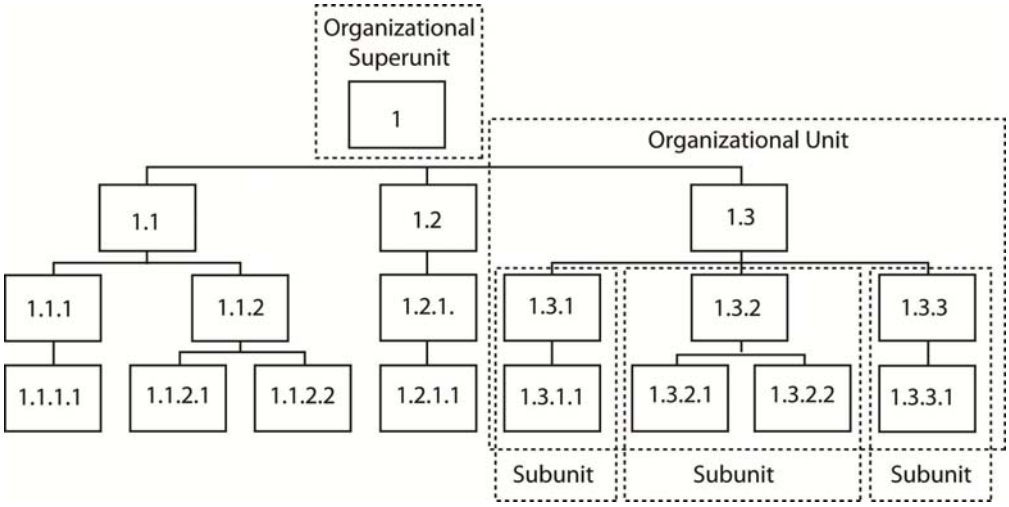

Figure 2: Organizational Unit, Subunit, and Superunit on an Organization Chart

When the scope of the appraisal is determined to be organization-wide (enterprise-wide), the appraisal team must determine which level of "organizational unit" should be interviewed and supply artifacts for each selected process area, goal, or practice.

The organizational scope consists of the organizational units that will be selected to provide examples (or instantiations) of practices used in appropriate contexts (the organizational unit, superunit, and subunit; the organizational scope; and the reference model scope).

A. For those process areas, goals, or practices identified as pertaining only to the organizational subunit level, the subunit must provide evidence for all of the practices.

B. For those process areas, goals, or practices identified as pertaining to both the superunit and subunit levels, both the superunit and appropriate subunit must provide evidence for all of the practice instantiations, unless one or more of these practices do not apply to a particular subunit. For all practices that do not apply to the subunit, another suitable subunit must be found to provide evidence for those practices.

C. For those process areas, goals, or practices identified as pertaining only to the superunit level, the subunits need not provide evidence for any of the practices. However, for organizational alignment between strategic objectives and operational practices, it may be useful to understand the level of practice instantiation in the subunits within the hierarchy of the superunit.

Clearly, a broadly-defined organizational superunit (e.g., a multinational enterprise) will require significantly more objective evidence to be collected and analyzed than will a narrowly defined organizational unit (e.g., a specific department within a specific business unit at a single geographical location).

The organizational unit to which appraisal results are attributed should be described accurately in all statements made by the appraisal team and sponsor. It is the responsibility of the appraisal team leader to understand the larger organizational context in which the appraised organizational unit resides. This understanding is aided by familiarity with the organization's structure, services and their associated asset relationships, performance of operational risk management, and information systems security or business continuity functions that may affect the interpretation of appraisal. The organizational unit should be documented in the clearest terms possible within the context of the organizational structure. It is often difficult to specify unambiguous boundaries without resorting to naming individual people in some organizations. Information about the organizational unit should be documented in a way that allows future appraisal sponsors to replicate (to the extent possible) the organizational unit that has been appraised. This information should be in the appraisal plan and used (in summary form if needed) in briefing the appraisal team and appraisal participants.

Reference Model Scope

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

The model scope is determined by selecting specific CERT-RMM process areas. Process areas should be chosen based on the objectives and business case for the appraisal and in consideration of other appraisal requirements.

There are no firm rules about the minimum or maximum number of process areas that should be selected for inclusion in the model scope. Care should be taken to select as many process areas as necessary to achieve the appraisal objectives, but few enough so that appraisal conduct and progress in acting on appraisal results can be demonstrated in a reasonable time frame for the sponsor and key stakeholders. If the appraisal requirements call for a large number of process areas, then a time-phased, incremental approach should be considered. There are a number of approaches for determining reference model scope.

- targeted improvement roadmaps (TIR)—This term designates a specific collection of CERT-RMM process areas that serve a particular appraisal (and improvement) objective. An organization could declare a TIR to represent its unique appraisal requirements. Industry groups might establish TIRs to represent their specific operational resilience concerns or to address an industry initiative or new regulatory mandate. Also, an organization could establish TIRs to conduct an appraisal on specific tiers of suppliers or external entities and use the TIRs and appraisal results to support the evaluation, selection, and monitoring of those entities.
- practice-level scope—This enables the model scope to be limited to selected specific and generic practices within a process area. This option does not have to be applied to all process areas when establishing the model scope, but it may be appropriate for one or more process areas to address specific appraisal requirements. This scoping option may be useful in the early phases of an appraisal effort, in response to very narrow objectives, or to be consistent with the span of influence of the appraisal sponsor. Note that this scoping option is NOT allowed for a class A appraisal, which is the focus of this report. Practice-level scoping will be covered in more detail in a future report on CERT-RMM CAM class B and class C appraisals.
- asset-level scope—Because CERT-RMM addresses four asset types—people, information, technology, and facilities—the model scope of the appraisal effort could be focused on one or more process areas that could be tailored to focus on one or more asset types. For example, if the Asset Definition and Management (ADM) process area is chosen, the scope of application of this process area could be limited to the “information” asset. Some process areas are already bound by an asset scope. These include Human Resource Management and People Management (people), Knowledge and Information Management (information), Technology Management (software, systems, and hardware), and Environmental Control (facilities). This option may be useful depending on certain appraisal requirements or the appraisal strategy, or it may be used to tailor the model scope to best fit the span of influence of the appraisal sponsor.

  For example, an organization may limit the asset scope for Phase 1 of a multiphased appraisal to information and technology assets only. This is consistent with the span of influence of the appraisal sponsor and with the immediate appraisal requirement to assess information

security. If the model scope for the appraisal includes the ADM process area, for Phase 1 of the effort, ADM will be applied to information and technology assets only.

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

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

Figure 3 shows the relationship of the four model scope options.

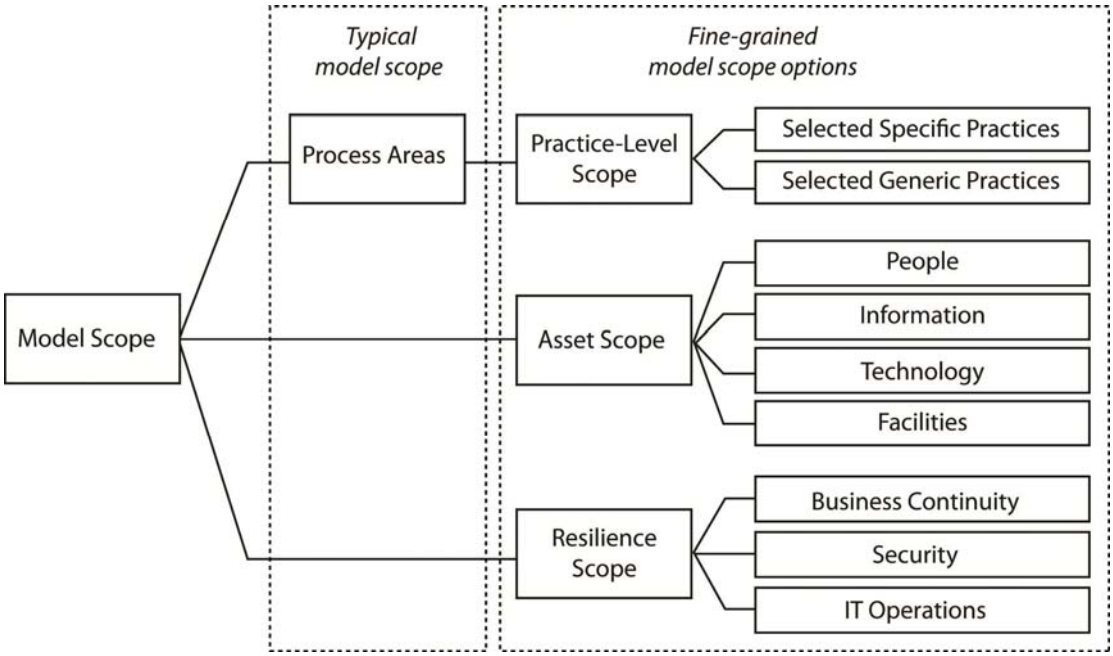

Figure 3: Reference Model Scope Options

If the Conduct Appraisal phase (see Phase 2) is to be performed using incremental subsets of the organizational unit or the reference model, the appraisal plan must identify the organizational scope and appraisal reference model scope for each increment.

A requirement of the class A method is that the Conduct Appraisal phase must be completed within 90 days; therefore, delta appraisals are not permitted. A delta appraisal is defined as a second appraisal performed on a subset of an original appraisal's reference model scope after correcting weaknesses reported in the previous appraisal, and then combining the results of the second appraisal with the results of the parts of the first appraisal that were not investigated in the second appraisal to produce new results.

Table 10 summarizes the Determine Appraisal Scope activity.

Table 10: Analyze Requirements: Determine Appraisal Scope

Process/Activity	Required Practices
1.1 Analyze Requirements	
1.1.3 Determine Appraisal Scope	The appraisal team leader, in conjunction with the appraisal sponsor and/or the sponsor's designee, shall • determine and document the reference model scope and representation to be used for the appraisal (CERT-RMM has continuous representation only) • determine and document the organizational units to be appraised • determine and document the organizational scope of the appraisal • identify and document the names of individuals who will participate in the appraisal

1.1.4 Determine Outputs

This activity identifies the specific appraisal outputs to be produced. Some outputs are expected, and additional outputs can be tailored to meet the business needs of the sponsor.

This process obtains information to answer the following questions:

- What findings will be generated during the appraisal?
- Will a final report be written to document appraisal results?
- Will recommendations on how to address specific findings be generated and reported?

The sponsor shall receive the appraisal record (expected output), which includes final findings, including documented statements of strengths and weaknesses for every CERT-RMM goal included in the scope of the appraisal.

The sponsor may also request that other products be generated as appraisal outputs. Typical products that might be requested and tailored include

- appraisal final report (written or oral presentations)
- recommendations for taking action on the appraisal results
- process improvement action plan

Satisfaction of a CERT-RMM goal is pass/fail (binary) and is directly related to the extent of practice implementation throughout the organizational scope of the appraisal. Goal satisfaction ratings for both specific goals and generic goals of the PAs within the scope of the appraisal are a minimum requirement for a class A appraisal. Goal satisfaction criteria are explained more fully in Section 2.6 of this report. Capability level ratings are optional.

Table 11 summarizes this activity.

Table 11: Analyze Requirements: Determine Outputs

Process/Activity	Required Practices
1.1 Analyze Requirements	
1.1.4 Determine Outputs	The appraisal team leader or designee shall • review required CERT-RMM class A capability appraisal outputs with the appraisal sponsor • review and select optional CERT-RMM class A capability appraisal outputs with the appraisal sponsor • determine the recipients of appraisal outputs based on sponsor instructions

1.1.5 Obtain Commitment to Appraisal Input

The appraisal sponsor formally approves the appraisal input, and this set of information is placed under change management (refer to SCAMPI-MDD V1.2 for the parameters and limits that may be included in the appraisal input). An appraisal team leader's ability to build and maintain commitment from the sponsor and the members of the sponsoring organization is a major factor contributing to the success of the appraisal. The process of understanding the requirements and constraints should yield a series of agreements that serve as inputs to the appraisal plan.

The appraisal team leader and the sponsor should have, at a minimum, a verbal agreement on the objectives, constraints, scope, and outputs, and these agreements should be documented in some way. The appraisal input may serve as a draft of the appraisal plan. The formality of agreements may range from simple meeting minutes and records of interaction with the appraisal sponsor, maintained by the appraisal team leader, to a more formal (signed) memorandum of understanding or other vehicle that documents agreements, provides traceability, and serves as a basis for future activities. It is expected that the appraisal plan will be used to formally document important issues from the appraisal input.

Table 12 summarizes this activity.

Table 12: Analyze Requirements: Obtain Commitment to Appraisal Input

Process/Activity	Required Practices
1.1 Analyze Requirements	
1.1.5 Obtain Commitment to Appraisal Input	The appraisal team leader or designee shall • record required information in the appraisal input • obtain sponsor approval of the appraisal input • manage changes to the appraisal input, obtaining sponsor approval of changes

1.2 Develop Appraisal Plan

The purpose of this process is to develop and document an appraisal plan that reflects the results of appraisal planning processes, including the requirements, agreements, estimates, appraisal risks, method tailoring, and practical considerations (e.g., schedules, logistics, and contextual information about the organization) associated with the appraisal. Ultimately the appraisal team leader obtains and records the sponsor's approval of the appraisal plan.

Skilled appraisal team leaders effectively develop and use outputs from the other Planning and Preparation phase activities to achieve clarity of the shared vision necessary to make the tradeoffs and decisions resulting in a final plan. Experienced appraisal team leaders leverage data, templates, and work products (developed through their own experience) to improve the completeness and effectiveness of the appraisal plan. Leaders recognize the return on investment that will be achieved through smooth and efficient appraisals that build upon past experience.

In some applications, planning templates and procedures used in the organization can be adapted to the needs of the appraisal. This approach aids communication and fosters local ownership of the process.

A structured planning workshop may benefit organizations with limited appraisal experience. Such a workshop is a valuable opportunity to discover appraisal risks as well as identify mitigation strategies.

The appraisal input identified in Section 1.1.5 includes the key appraisal requirements and strategic objectives, which require sponsor visibility and change control approval. The appraisal plan includes this information as well as the tactical planning details necessary to implement and satisfy appraisal objectives.

This process comprises six activities summarized in Table 13 and described below.

Table 13: Develop Appraisal Plan

Process/Activity	Required Practices
1.2 Develop Appraisal Plan	
1.2.1 Tailor Method	The appraisal team leader or designee shall • review and select tailoring options within each activity • ensure that the tailoring decisions are self-consistent and that they are appropriate in light of the appraisal objectives and constraints • document the tailoring decisions made
1.2.2 Identify Needed Resources	The appraisal team leader or designee shall • identify appraisal team members • identify appraisal participants • identify equipment and facilities • identify other appraisal resources needed • document resource decisions in the appraisal plan
1.2.3 Determine Cost and Schedule	The appraisal team leader or designee shall • estimate the duration of key events as a basis for deriving a comprehensive schedule • estimate the effort required for the people participating in the appraisal • estimate the costs associated with using facilities and equipment as appropriate • estimate the costs for incidentals (e.g., travel, lodging, and meals) as appropriate • document a detailed schedule in the appraisal plan • document detailed cost estimates in the appraisal plan
1.2.4 Plan and Manage Logistics	The appraisal team leader or designee shall • document logistical schedules and dependencies • maintain communication channels for providing status • assign responsibilities for tracking logistical issues
1.2.5 Document and Manage Appraisal Risks	The appraisal team leader or designee shall • identify appraisal risks • develop mitigation plans for key appraisal risks and implement these plans as necessary • keep the appraisal sponsor and other stakeholders informed of the appraisal risk status
1.2.6 Obtain Commitment to Appraisal Plan	The appraisal team leader or designee shall • document the appraisal plan • review the appraisal plan with the sponsor and secure the sponsor's approval • provide the appraisal plan to relevant stakeholders for review

1.2.1 Tailor Method

Method tailoring is directly related to organizational scope and appraisal reference model scope decisions. Most of the allowable tailoring options flow logically from these decisions when taken in the context of the appraisal objectives and constraints. Tailoring decisions may also result in appraisal risks. Typical tailoring choices that may affect appraisal planning include

- assigning mini-teams (two or three members of the larger appraisal team) to focus on a specific thread in the model such as risk management, service continuity, or other process area grouping
- using data collection approaches including supporting work aids and tools (e.g., use of video conference, teleconference, or other similar technology to conduct interviews, conducting parallel interview sessions with a minimum of two team members, and use of a Practice Implementation Indicator (PII) database or other information repository)
- using discovery-based appraisal[2] instead of verification-based appraisal
- using verification and validation approaches including supporting work aids and tools (e.g., mini-team verification of practices at the instantiation level)
- selecting optional appraisal outputs (e.g., preliminary findings focused on organizational units, model disciplines such as information security or business continuity, or a capability level target for improvement)
- documenting strengths and nonmodel findings (i.e., observations from team members that are ancillary to the reference model used in the appraisal)
- performing optional activities (e.g., conducting executive session, planning for next steps, or collecting lessons learned)

Experienced appraisal team leaders provide a well-defined approach to ensure that the appraisal objectives are achieved in an efficient and effective manner. Experienced sponsors require a well-defined approach to ensure an acceptable level of risk in meeting objectives within the constraints. The appraisal plan documents the method-tailoring decisions and their rationale, as well as the associated method variations and techniques that will be employed.

Table 14 summarizes this activity.

Table 14: Develop Appraisal Plan: Tailor Method

Process/Activity	Required Practices
1.2 Develop Appraisal Plan	
1.2.1 Tailor Method	The appraisal team leader or designee shall • review and select tailoring options within each activity • ensure that the tailoring decisions are self-consistent and that they are appropriate in light of the appraisal objectives and constraints • document the tailoring decisions made

[2] An appraisal in which limited objective evidence is provided by the appraised organizational unit prior to the appraisal, requiring the appraisal team to probe and uncover a majority of the objective evidence necessary to obtain sufficient coverage of reference model practices. Discovery-based appraisals typically involve substantially greater appraisal team effort than verification-based appraisals, in which much of the objective evidence is provided by the appraised organizational unit.

1.2.2 Identify Needed Resources

Appraisal resources are typically defined early in the appraisal planning process. Identifying resources goes hand in hand with estimating appraisal cost and schedule. Tradeoffs and refinement of resource needs are routinely made in light of the appraisal objectives and constraints.

The appraisal sponsor or designee may identify candidate appraisal team members and appraisal participants. Review of the organizational unit structure or other site-specific information can be useful for resource identification. Initially, participants can be specified by role or responsibility, with specific names to be determined later.

The use of existing equipment and facilities is often negotiated with the organizational unit where the appraisal activities will be performed, but sometimes equipment and facilities must be acquired. The availability of computing resources, such as computers, printers, and networks, is a key consideration that should be planned and understood. Access to special tools or applications may also be needed. A room for dedicated use by the appraisal team is usually necessary for private discussions and to protect the confidentiality of appraisal data. Ideally, this room is separate from the other rooms where interview sessions are held.

Table 15 summarizes this activity.

Table 15: Develop Appraisal Plan: Identify Needed Resources

Process/Activity	Required Practices
1.2 Develop Appraisal Plan	
1.2.2 Identify Needed Resources	The appraisal team leader or designee shall • identify appraisal team members • identify appraisal participants • identify equipment and facilities • identify other appraisal resources needed • document resource decisions in the appraisal plan

1.2.3 Determine Cost and Schedule

Cost and schedule may be developed from the top down based on sponsor objectives and constraints, from the bottom up based on results of other planning and preparation processes and activities, or more generally using a combination of the two approaches. Scheduling the events and activities of the appraisal is an ongoing logistical task that requires the coordination of many different groups of individuals. Determining and communicating a schedule for the appraisal, and maintaining ongoing visibility as the details are determined, is the primary responsibility of the appraisal team leader. It may be useful to assign a coordinator to provide support for this activity.

Schedule constraints are determined by balancing the needs of the sponsor for appraisal outputs of a specified quality fulfilling a specified purpose against the resources available to conduct the appraisal. Schedule and cost must be considered for the entire time frame of the appraisal activities.

Effort estimates should be developed not only for the appraisal team, but also for the expected participants within the organizational unit (e.g., interviewees, respondents to administered data elicitation instruments, attendees at briefings, and support staff).

Organizational costs for preparing and supporting multiple appraisals can be reduced by gathering and maintaining objective evidence for each similar type of practice instantiation. Some of the objective evidence for one part of the appraisal may also satisfy another part of the appraisal. The appraisal should be carefully planned to take advantage of synergies in data collection. This approach enables the ready availability and reuse of objective evidence for subsequent appraisals of any class, providing the evidence is current and applicable to the practices being evaluated. In addition it provides an effective mechanism for monitoring the process implementation and improvement progress of the organizational unit.

While the schedule for the appraisal is shared with a fairly wide audience, the cost of the appraisal (or elements within the appraisal) is often shared more selectively, due to the potentially sensitive nature of this information.

Table 16 summarizes this activity.

Table 16: Develop Appraisal Plan: Determine Cost and Schedule

Process/Activity	Required Practices
1. 2 Develop Appraisal Plan	
1.2.3 Determine Cost and Schedule	The appraisal team leader or designee shall • estimate the duration of key events as a basis for deriving a comprehensive schedule • estimate the effort required for the people participating in the appraisal • estimate the costs associated with using facilities and equipment as appropriate • estimate the costs for incidentals (e.g., travel, lodging, and meals) as appropriate • document a detailed schedule in the appraisal plan • document detailed cost estimates in the appraisal plan

1.2.4 Plan and Manage Logistics

The logistical details of the appraisal are negotiated and documented. The appraisal team leader, supported by an organizational unit coordinator (if available), manages planning tasks that document and communicate logistical arrangements. Checklists and action item tracking mechanisms are important tools for managing these tasks. Table 17 summarizes this activity.

Table 17: Develop Appraisal Plan: Plan and Manage Logistics

Process/Activity	Required Practices
1. 2 Develop Appraisal Plan	
1.2.4 Plan and Manage Logistics	The appraisal team leader or designee shall • document logistical schedules and dependencies • maintain communication channels for providing status • assign responsibilities for tracking logistical issues

1.2.5 Document and Manage Appraisal Risks

As with any project that has dependencies among events, people, and other resources, risk management is an important ingredient to success. The appraisal team leader is responsible for documenting and communicating appraisal risks and associated mitigation plans to the sponsor and appraisal team members. Table 18 summarizes this activity.

Table 18: Develop Appraisal Plan: Document and Manage Appraisal Risks

Process/Activity	Required Practices
1. 2 Develop Appraisal Plan	
1.2.5 Document and Manage Appraisal Risks	The appraisal team leader or designee shall • identify appraisal risks • develop mitigation plans for key appraisal risks and implement these plans as necessary • keep the appraisal sponsor and other stakeholders informed of the appraisal risk status

1.2.6 Obtain Commitment to Appraisal Plan

Formal sponsor commitment to the appraisal plan is obtained. The appraisal plan constitutes a contract between the appraisal sponsor and the appraisal team leader, so it is vital that this agreement be formal.

While sponsor visibility into the appraisal plan is necessary, revisions are typically low-level implementation details and do not ordinarily require sponsor reapproval. This low level of change is in contrast to the appraisal input, which contains strategic, key appraisal requirements, objectives, and constraints. Revisions to the appraisal input must be approved by the sponsor. In practical use, the appraisal input is often packaged as a component of the appraisal plan, and a single sponsor signature can serve as approval for both. The separation of the appraisal input and the appraisal plan is intended to provide an appropriate level of sponsor visibility and approval, while leaving appraisal team leaders the flexibility to refine the low-level details necessary to complete thorough appraisal planning. Table 19 summarizes this activity.

Table 19: Develop Appraisal Plan: Obtain Commitment to Appraisal Plan

Process/Activity	Required Practices
1. 2 Develop Appraisal Plan	
1.2.6 Obtain Commitment to Appraisal Plan	The appraisal team leader or designee shall • document the appraisal plan • review the appraisal plan with the sponsor and secure the sponsor's approval • provide the appraisal plan to relevant stakeholders for review

1.3 Select and Prepare Team

This process ensures that an experienced, trained, and appropriately qualified team is available and prepared to execute the appraisal process. The appraisal team is a cohesive unit of trained and capable professionals, each of whom must meet stringent qualifications. An appraisal team leader is selected to plan and manage the performance of the appraisal, delegate appraisal tasks to team

members, and ensure adherence to CERT-RMM class A appraisal requirements. Appraisal team members are selected based on defined criteria for experience, knowledge, and skills to ensure an efficient team capable of satisfying the appraisal objectives. Training is provided to ensure proficiency in the appraisal reference model and appraisal method.

This process is composed of three activities summarized in Table 20 and described below.

Table 20: Select and Prepare Team

Process/Activity	Required Practices
1.3 Select and Prepare Team	
1.3.1 Identify Appraisal Team Leader	The appraisal sponsor or designee shall • select an authorized CERT-RMM lead appraiser to serve as the appraisal team leader • verify the qualifications of the appraisal team leader (experience, knowledge, and skills)
1.3.2 Select Team Members	The appraisal team leader or designee shall • select individual team members who meet the minimum criteria for individual team members • select individual team members who collectively meet the minimum criteria for the team as a whole • document the qualifications and responsibilities of team members in the appraisal plan
1.3.3 Prepare Team	The appraisal team leader or designee shall • ensure that appraisal team members have received appraisal reference model training • provide appraisal method training to appraisal team members or ensure that they have already received it • establish team building and team norms • provide an orientation to team members on appraisal objectives, plans, and their assigned roles and responsibilities

1.3.1 Identify Appraisal Team Leader

The appraisal sponsor is responsible for selecting an appraisal team leader who has the appropriate experience, knowledge, and skills to take responsibility for and lead the appraisal. The appraisal team leader is responsible for ensuring that the appraisal is conducted in accordance with CERT-RMM class A appraisal requirements (Section 1.1) and with tailoring approaches to meet appraisal objectives and constraints within allowable bounds defined by the method.

There can be only one official appraisal team leader on any given appraisal. The appraisal team leader has sole discretion to delegate important tasks to appraisal team members but cannot delegate leadership responsibility or ultimate responsibility for the successful completion of the appraisal.

Appraisal team leader responsibilities are defined and described throughout this report. An overview of these responsibilities includes the following:

- Confirm the sponsor's commitment to proceeding with the appraisal.
- Ensure the appraisal participants are briefed on the purpose, scope, and approach of the appraisal.

- Ensure the appraisal team members have the appropriate experience, knowledge, and skills in the CERT-RMM reference model and in RMM-CAM.
- Ensure adequate planning and preparation of appraisal team members.

Table 21 summarizes this activity.

Table 21: Select and Prepare Team: Identify Appraisal Team Leader

Process/Activity	Required Practices
1.3 Select and Prepare Team	
1.3.1 Identify Appraisal Team Leader	The appraisal sponsor or designee shall • select an authorized CERT-RMM lead appraiser to serve as the appraisal team leader • verify the qualifications of the appraisal team leader (experience, knowledge, and skills)

1.3.2 Select Team Members

This activity involves identifying available personnel, assessing their qualifications, and selecting them to become appraisal team members. The minimum acceptable team size for a CERT-RMM class A appraisal is four people (including the appraisal team leader). The maximum recommended team size is nine, but a balance between the scope of the appraisal and the size of the team should be considered.

All team members are required to complete the Introduction to the CERT Resilience Management Model course before conducting the appraisal.

Team members should not be managers of any of the selected organizational units or support groups or be within the direct supervisory chain of any of the anticipated interviewees if at all possible. It is the responsibility of the appraisal team leader to identify and manage potential or perceived conflicts of interest that may impair an appraisal team's ability to function objectively. The appraisal team leader must use professional judgment and evaluate potential conflicts, review them with the appraisal sponsor, and ensure detailed documentation in the appraisal plan reflects the strategies used to mitigate the risks of any conflicts.

Appraisal team members are selected to provide a diverse set of qualified professionals with the appropriate experience, knowledge, and skills to make reasoned judgments regarding implementation of the appraisal reference model. The accuracy and credibility of the appraisal results depends greatly on the capability, qualifications, and preparation of the appraisal team members. The team must, in aggregate, have experience in the operational areas and functional domains being appraised.

Suggested criteria for the composition of the appraisal team should include the following:

- The team (as a group) should have an average of three years of experience in the specific discipline (security, business continuity, IT operations) to be covered in the appraisal, and the team's total experience should include at least six years in each of the disciplines in CERT-RMM.
- Staff and project management experience of at least three years is highly desirable.

- Team member certifications in domain-specific areas of the reference model are highly desirable. Examples of organizations providing certification in CERT-RMM disciplines include (but are not limited to)
  - ISACA (CISA, CISM, CGEIT, CRISC)
  - ISC2 (CISSP, CAP)
  - SANS Institute (GIAC, GSEC)
  - Disaster Recovery Institute (CBCP, MBCP)
  - Business Continuity Institute (CBCI, MBCI)
  - itSMF (ITIL)
  - PMI (PMP)
- Good oral and written communications skills are desirable, as well as the ability to facilitate the free flow of communication, the ability to perform as a team player, and negotiation skills.

The appraisal team leader is wholly responsible for the appropriate composition of the appraisal team to meet the appraisal requirements.

Table 22 summarizes this activity.

Table 22: Select and Prepare Team: Select Team Members

Process/Activity	Required Practices
1.3 Select and Prepare Team	
1.3.2 Select Team Members	The appraisal team leader or designee shall • select individual team members who meet the minimum criteria for individual team members • select individual team members who collectively meet the minimum criteria for the team as a whole • document the qualifications and responsibilities of team members in the appraisal plan

1.3.3 Prepare Team

The appraisal team leader is responsible for ensuring that appraisal team members are sufficiently prepared to perform the planned appraisal activities. This preparation includes ensuring team members are familiar with the appraisal reference model, the appraisal method, the appraisal plan, organizational data and characteristics, and the tools and techniques to be used during the appraisal. Roles and responsibilities are assigned for appraisal tasks. Team building exercises are used to practice facilitation skills and achieve a common understanding of team and appraisal objectives and how they will be satisfied.

All team members are expected to observe strict rules for confidentiality, the protection of proprietary or sensitive data, and the nonattribution of information to appraisal participants. Nondisclosure statements are often used to formalize these understandings.

Team members who have previously received SCAMPI with CMMI team training or SCAMPI with People CMM team training are NOT automatically qualified to participate on a CERT-RMM appraisal without first attending the Introduction to the CERT Resilience Management Model course.

The appraisal team leader is required to understand the nature of the training that all team members have received and the adequacy of that training for the appraisal.

Table 23 summarizes this activity.

Table 23: Select and Prepare Team: Prepare Team

Process/Activity	Required Practices
1.3 Select and Prepare Team	
1.3.3 Prepare Team	The appraisal team leader or designee shall • ensure that appraisal team members have received appraisal reference model training • provide appraisal method training to appraisal team members or ensure that they have already received it • establish team building and team norms • provide an orientation to team members on appraisal objectives, plans, and their assigned roles and responsibilities

1.4 Obtain and Inventory Initial Objective Evidence

The purpose of this process is to obtain information that facilitates site-specific preparation and an understanding of the implementation of model practices across the organizational units that are the focus of the appraisal. The appraisal team identifies potential issues, gaps, and risks to aid in refining the appraisal plan. This process strengthens the appraisal team members' understanding of the organization's operations and processes. Note that a discovery-based appraisal is a tailoring option of a CERT-RMM class A capability appraisal. If this option is chosen, there may be limited objective evidence to inventory at this stage of the appraisal.

This process is composed of two activities summarized in Table 24 and described below.

Table 24: Obtain and Inventory Initial Objective Evidence

Process/Activity	Required Practices
1.4 Obtain and Inventory Initial Objective Evidence	
1.4.1 Obtain Initial Objective Evidence	The appraisal team leader or designee shall • obtain documentation reflecting the implementation of model practices from the appropriate organizational units included in the appraisal scope
1.4.2 Inventory Objective Evidence	The appraisal team leader or designee shall • examine the initial set of objective evidence provided by the appropriate organizational unit, unless a discovery-based appraisal has been selected • determine the extent to which additional information is needed for adequate coverage of model practices

1.4.1 Obtain Initial Objective Evidence

In this activity, the appraisal team leader requests detailed data on the implementation of practices in the organizational units specified in the appraisal scope. The appraisal team leader is free to specify the format to be used and the level of detail to be provided, knowing that anything that is not provided in advance must be collected later in the appraisal process. There are no minimum requirements set by the method with respect to completeness or detail in this initial data set. However, the effort required to conduct a CERT-RMM class A capability appraisal is a direct

function of the amount of data available to the team at the beginning of the process. Before the appraisal outputs can be created, the team must verify objective evidence for each instantiation of each practice within the scope of the appraisal.

During the appraisal, the appraisal team verifies and validates the objective evidence provided by the appraised organization to identify strengths and weaknesses relative to CERT-RMM. The data used for an appraisal correlates to the performance of one or more practices of the appraisal reference model, regardless of how the data is collected (using instruments such as questionnaires, reviewing documents, attending presentations, or conducting interviews). For every practice within the reference model scope of the appraisal, and for every instance of each practice, objective evidence is used as the basis for appraisal team determinations of the extent to which the practice is implemented. Indicators that substantiate practice implementation include the following:

- *direct* artifacts, which represent the primary tangible output of a practice. These artifacts are typically listed in the appraisal reference models as typical work products. One or more direct artifacts are necessary to verify the implementation of associated model practices.
- *indirect* artifacts, which represent artifacts that are a consequence of performing the practice, but do not necessarily represent the purpose for which it is performed. These artifacts are typically things like meeting minutes, review results, or written communications of status, and may also be listed as typical work products.
- *affirmations*, which are oral or written statements confirming the implementation of the practice. These statements are typically collected using interviews, questionnaires, or other means. Note that negative affirmations confirming the lack of implementation of a practice are possible.

Prior to the data collection activities carried out by the appraisal team, an initial data set is usually created by the appraised organizational units. This data set contains descriptions of the objective evidence available for the team to examine, complete with references to documentation and identification of the personnel who can provide relevant affirmations. The data set provides the baseline of objective evidence for the appraisal. Organizational units experienced in process improvement most likely have this type of data on hand, as they will have used it in the past to track their improvement progress. Organizational units not experienced in process improvement will need additional instruction, guidance, and coaching to prepare an artifact repository or work product catalog for use as initial objective evidence.

Artifacts may be obtained as hard copies, soft copies, or hyperlinks to where these documents reside in a web-based environment. If hyperlinks are used, the accessibility of artifacts via these links should be verified on-site before leaving the appraisal environment.

Table 25 summarizes this activity.

Table 25: Obtain and Inventory Objective Evidence: Obtain Initial Objective Evidence

Process/Activity	Required Practices
1.4 Obtain and Inventory Objective Evidence	
1.4.1 Obtain Initial Objective Evidence	The appraisal team leader or designee shall • obtain documentation reflecting the implementation of model practices from the appropriate organizational units included in the appraisal scope

1.4.2 Inventory Objective Evidence

The inventory of the initial data set provides critical new information for the overall planning of the appraisal and forms the basis for the detailed data collection plan that must be developed before the Conduct Appraisal phase (see Phase 2). The inventory of initial objective evidence at this stage is focused primarily on the adequacy and completeness of information and the implications for future data collection. The results of this activity are the primary basis for determining the extent to which the appraisal will be one of verification or discovery.

Table 26 summarizes this activity.

Table 26: Obtain and Inventory Objective Evidence: Inventory Objective Evidence

Process/Activity	Required Practices
1. 4 Obtain and Inventory Objective Evidence	
1.4.2 Inventory Objective Evidence	The appraisal team leader or designee shall • examine the initial set of objective evidence provided by the appropriate organizational unit, unless a discovery-based appraisal has been selected • determine the extent to which additional information is needed for adequate coverage of model practices

1.5 Prepare for Appraisal Conduct

The purpose of this process is to ensure readiness to conduct the appraisal, including confirmation of the availability of objective evidence, appraisal team commitment, logistics arrangements, risk status, and associated mitigation plans. At this stage of the process, there should be an initial plan that defines strategies for data collection.

This process is composed of three activities summarized in Table 27 and described below.

Table 27: Prepare for Appraisal Conduct

Process/Activity	Required Practices
1.5 Prepare for Appraisal Conduct	
1.5.1 Perform Readiness Review	The appraisal team leader or designee shall • determine whether the objective evidence for each instance of each practice in the appraisal scope is adequate for proceeding with the appraisal as planned • determine whether the appraisal team is prepared to conduct the appraisal • ensure the appraisal logistics (e.g., facilities, equipment, and participant availability) have been arranged and confirmed • review identified appraisal risks to determine status and impact of conducting the appraisal as planned • review the feasibility of the appraisal plan in light of data readiness, team readiness, logistics readiness, and overall appraisal risk
1.5.2 Prepare Data Collection Plan	The appraisal team leader or designee shall • determine participants for interviews • determine artifacts to be reviewed • determine presentations/demonstrations to be provided • determine team roles and responsibilities for data collection activities • document the data collection plan
1.5.3 Replan Data Collection	The appraisal team leader or designee shall • review the current inventory of objective evidence and determine model practices for which the objective evidence is inadequate relative to the appraisal plan • revise the data collection plan as necessary based on the appraisal status and availability of objective evidence • renegotiate the appraisal plan with the sponsor if the appraisal cannot proceed as planned

1.5.1 Perform Readiness Review

The readiness review is used to determine whether or not the appraisal team and appraised organization are ready to conduct the appraisal as planned. The readiness review addresses several aspects of readiness to conduct the appraisal: data readiness, team readiness, logistics readiness, and appraisal risk status. The readiness review results in a decision to continue as planned, replan or reschedule, or cancel the appraisal. The appraisal team leader and sponsor are responsible for the decision and for determining the conditions under which to proceed.

Table 28 summarizes this activity.

Table 28: Prepare for Appraisal Conduct: Perform Readiness Review

Process/Activity	Required Practices
1. 5 Prepare for Appraisal Conduct	
1.5.1 Perform Readiness Review	The appraisal team leader or designee shall • determine whether the objective evidence for each instance of each practice in the appraisal scope is adequate for proceeding with the appraisal as planned • determine whether the appraisal team is prepared to conduct the appraisal • ensure the appraisal logistics (e.g., facilities, equipment, and participant availability) have been arranged and confirmed • review identified appraisal risks to determine status and impact of conducting the appraisal as planned • review the feasibility of the appraisal plan in light of data readiness, team readiness, logistics readiness, and overall appraisal risk

1.5.2 Prepare Data Collection Plan

The data collection activities are tailored to meet the needs for objective evidence so that the extent of practice implementation can be determined. For practices that have objective evidence, a strategy for verifying that evidence is formulated. For practices that lack objective evidence, a strategy for discovering that evidence is formulated.

The data collection plan is typically embodied in a number of different artifacts used during the appraisal process. The data collection plan must specify contingencies to manage the risk of having insufficient data. For every instantiation of every model practice, the data collection plan must specify how, when, and by whom the objective evidence will be verified. For instantiations of model practices that have not been addressed in the initial objective evidence, the data collection plan must specify how the team intends to discover the presence or absence of objective evidence that characterizes the extent of implementation for that practice.

Table 29 summarizes this activity.

Table 29: Prepare for Appraisal Conduct: Prepare Data Collection Plan

Process/Activity	Required Practices
1. 5 Prepare for Appraisal Conduct	
1.5.2 Prepare Data Collection Plan	The appraisal team leader or designee shall • determine participants for interviews • determine artifacts to be reviewed • determine presentations/demonstrations to be provided • determine team roles and responsibilities for data collection activities • document the data collection plan

1.5.3 Replan Data Collection

The data collection plan is updated as required during the conduct of the readiness review or during the appraisal itself as objective evidence is found or as new sources of information are

uncovered. The activity described in this section refers to a more substantial change in the plan, which is expected to be a rare occurrence in practice. If during an appraisal the team discovers that their assumptions about the availability of objective evidence are substantially incorrect, the appraisal team leader may renegotiate the appraisal plan with the sponsor. This activity is not a substitute for tactical decisions about where and how to find objective evidence. The intent of this activity is to respond to a major gap between expected data and actual data.

When this activity must be employed to recover from an unrealistic expectation, the documentation reflecting the assumptions made during planning, as well as concrete facts about what is or is not available, are used to renegotiate with the appraisal sponsor. The need to renegotiate is one of the reasons why a formal, detailed appraisal plan, with the sponsor's signature, is a required artifact for the conduct of a CERT-RMM class A capability appraisal.

Table 30 summarizes this activity.

Table 30: Prepare for Appraisal Conduct: Replan Data Collection

Process/Activity	Required Practices
1. 5 Prepare for Appraisal Conduct	
1.5.3 Replan Data Collection	The appraisal team leader or designee shall • review the current inventory of objective evidence and determine model practices for which the objective evidence is inadequate relative to the appraisal plan • revise the data collection plan as necessary based on the appraisal status and availability of objective evidence • renegotiate the appraisal plan with the sponsor if the appraisal cannot proceed as planned

2 Conduct Appraisal

The Conduct Appraisal phase (see Table 31) has six processes: Prepare Participants, Examine Objective Evidence, Document Objective Evidence, Verify Objective Evidence, Validate Preliminary Findings, and Generate Appraisal Results. Each of these processes has additional tasks and activities explained in subsequent sections.

Table 31: Conduct Appraisal

Process	Activity
2.1 Prepare Participants	2.1.1 Conduct Participant Briefing
2.2 Examine Objective Evidence	2.2.1 Examine Objective Evidence[3]
2.3 Document Objective Evidence	2.3.1 Take/Review/Tag Notes
	2.3.2 Record Presence/Absence of Objective Evidence
	2.3.3 Document Practice Implementation
	2.3.4 Review and Update the Data Collection Plan
2.4 Verify and Validate Objective Evidence	2.4.1 Verify Objective Evidence
	2.4.2 Characterize Implementation of Model Practices
2.5 Validate Preliminary Findings	2.5.1 Validate Preliminary Findings
2.6 Generate Appraisal Results	2.6.1 Derive Findings and Rate Goal
	2.6.2 Determine Process Area Capability Level
	2.6.3 Determine Capability Profile
	2.6.4 Document Appraisal Results

2.1 Prepare Participants

The purpose of this process is to ensure that appraisal participants are appropriately informed of the appraisal process, purpose, and objectives and are available to participate in the appraisal process.

This process is composed of one activity summarized in Table 32 and described below.

Table 32: Prepare Participants

Process/Activity	Required Practices
2.1 Prepare Participants	
2.1.1 Conduct Participant Briefing	The appraisal team leader or designee shall • brief appraisal participants on the appraisal process • provide orientation to appraisal participants on their roles in the appraisal

2.1.1 Conduct Participant Briefing

Members of the organization who participate in the appraisal must be informed of their role and the expectations of the sponsor and appraisal team. This communication is typically accomplished

[3] This activity combines SCAMPI MDD V1.2 activities 2.2.1 Examine Objective Evidence from Documents and 2.2.2 Examine Objective Evidence from Interviews.

through a briefing in which the appraisal team leader provides an overview of the appraisal process, purpose, and objectives. Specific information about the scheduled events and the locations where they occur is also communicated during this presentation, as well as through ongoing contact between the organizational unit coordinator and the members of the organizational unit.

Table 33 summarizes this activity.

Table 33: Prepare Participants: Conduct Participant Briefing

Process/Activity	Required Practices
2.1 Prepare Participants	
2.1.1 Conduct Participant Briefing	The appraisal team leader or designee shall • brief appraisal participants on the appraisal process • provide orientation to appraisal participants on their roles in the appraisal

2.2 Examine Objective Evidence

Examination of the objective evidence includes reviewing the documents, interview notes, direct observation or practice implementation, practice implementation indicator (PII) database, or survey questionnaires to determine if the collected evidence is acceptable to support one or more specific practice instantiations. Examining information about the practices implemented in the organization is required to relate the resultant data to the appraisal reference model. The efficient collection of objective evidence results from carefully creating and executing the data collection plan. Examination of data should be performed in accordance with the data collection plan (see Section 1.5.2). Effective contingency planning and the use of work aids to monitor progress are key points to consider in the event that the objective evidence is not acceptable to support one or more specific practice instantiations. The team must be able to focus on examining the most relevant information available, rather than be distracted by a mission to find new evidence.

When reviewing objective evidence, it may be helpful to consider combining the examination of the evidence with the documentation of the evidence (see Section 2.3) for efficiency in people-hours and as a means of creating or adding to a process asset library for future use.

This process is composed of one activity summarized in Table 34 and described below.

Table 34: Examine Objective Evidence: Examine Objective Evidence

Process/Activity	Required Practices
2.2 Examine Objective Evidence	
2.2.1 Examine Objective Evidence	The appraisal team shall • establish and maintain an inventory of documents used as sources of objective evidence • review information obtained from documents and determine if it is acceptable as objective evidence • determine the model practices corresponding to the objective evidence obtained from documents • determine the portions of the organizational unit that correspond to the objective evidence obtained from documents • refine the data collection plan to determine the objective evidence that must be obtained from interview participants • conduct interviews to obtain information that may be used as objective evidence • review information obtained from interviews and determine if it is acceptable as objective evidence • determine the model practices corresponding to the objective evidence obtained from interviews • determine the portions of the organizational unit that correspond to the objective evidence obtained from interviews

2.2.1 Examine Objective Evidence

A substantial portion of the data used by appraisal team members is derived from documents they review. Document review is an effective means of gaining detailed insight about the practices in use in the organization. However, without a clear focus on the data being sought, document review can consume a great deal of time as team members sometimes attempt to read everything in hopes that something useful will be discovered. Instruments, such as questionnaires and objective evidence descriptions as well as presentation materials, can provide documented objective evidence.

Interviews are used to obtain oral affirmations related to the implementation of processes within the organizational scope of the appraisal. The appraisal team uses interviews to understand how the processes are implemented and to probe areas where additional coverage of model practices is needed. Interviews are a required and necessary component of a CERT-RMM class A capability appraisal. All interviews must include at least two members of the appraisal team designated by the appraisal team leader. The rules of confidentiality and the expected use of appraisal data must be communicated to every interviewee. The criteria for the amount of orally affirmed objective evidence to be collected are described in Activity 2.4.1, Verify Objective Evidence.

Table 35 summarizes this activity.

Table 35: Examine Objective Evidence: Examine Objective Evidence

Process/Activity	Required Practices
2.2 Examine Objective Evidence	
2.2.1 Examine Objective Evidence	The appraisal team shall • establish and maintain an inventory of documents used as sources of objective evidence • review information obtained from documents and determine if it is acceptable as objective evidence • determine the model practices corresponding to the objective evidence obtained from documents • determine the portions of the organizational unit that correspond to the objective evidence obtained from documents • refine the data collection plan to determine the objective evidence that must be obtained from interview participants • conduct interviews to obtain information that may be used as objective evidence • review information obtained from interviews and determine if it is acceptable as objective evidence • determine the model practices corresponding to the objective evidence obtained from interviews • determine the portions of the organizational unit that correspond to the objective evidence obtained from interviews

2.3 Document Objective Evidence

The purpose of documenting the objective evidence is to create a lasting record of the information gathered by the appraisal team. The appraisal team observes, hears, and reads information that is transformed into notes, and then into practice characterizations, and then into preliminary findings. The objective evidence forms the foundation for a successful appraisal and must be rigorously documented to provide an accurate reflection of the organization's capability in relation to the appraisal model, and it must be used as a basis for comparisons within and across organizations. Documentation of the evidence creates residual appraisal assets that can be used as the basis for subsequent appraisals and for monitoring process improvement activities and progress. Appraisal results are also useful to the appraisal sponsor in decision analysis and may be used in the context of the sponsor's business objectives.

Several high-level tools and techniques can assist in this process as follows:

- Work aids like wall charts, spreadsheet programs, and automated database tools may be used to help track the status of data collection.
- Assigning specific PAs or specific tasks to mini-teams (pairs or triplets of team members) is a common practice.
- Time management is a critical skill for this activity. Explicitly reviewing the effort spent, in real time, is useful for focusing the team.
- Team norms regarding techniques for managing debates and divergent views are important and should be made explicit well in advance.

This process is composed of four activities summarized in Table 36 and described below.

Table 36: Document Objective Evidence

Process/Activity	Required Practices
2.3 Document Objective Evidence	
2.3.1 Take/Review/Tag Interview Notes	The appraisal team shall • record notes obtained from objective evidence data-gathering sessions • relate notes to corresponding practices in the appraisal reference model
2.3.2 Record Presence/Absence of Objective Evidence	The appraisal team shall • for each instantiation, record the presence or absence of objective evidence collected for each reference model practice within the appraisal scope
2.3.3 Document Practice Implementation	The appraisal team shall • document gaps in the implemented processes relative to appraisal reference model practices
2.3.4 Review and Update Data Collection Plan	The appraisal team shall • review the inventory of objective evidence collected and the data collection plan to determine what additional objective evidence is still needed for adequate coverage of the appraisal reference model scope • revise the data collection plan to obtain additional objective evidence for instances where available data are inadequate to judge the implementation of appraisal reference model practices • identify priorities for the upcoming data collection events and reevaluate the feasibility of the schedule in light of the current state of the objective evidence

2.3.1 Take/Review/Tag Interview Notes

The most basic representation of appraisal data is found in the notes taken by individual team members. These notes are reviewed and are typically tagged or otherwise processed before their content is transformed into other lasting representations. The presence, absence, and/or appropriateness of objective evidence is then judged and recorded based on the data collected. The scheme by which this set of records is produced is an important implementation choice made by the appraisal team leader, and it must be well understood by the team. Gaps in the implemented practices are also recorded in a consistent manner that ensures traceability. Finally, the data collection plan is reviewed in light of the changes in the set of data available to the team and the remaining data needed to support reliable rating judgments.

Every team member present must take notes during interviews and presentations. These notes must cover all areas investigated during the interview and are not limited to the PAs assigned to the individual team member (i.e., everybody takes notes on everything). The raw notes taken during an appraisal are treated as confidential information and may not be provided to any person outside of the appraisal team. Team members are typically required to destroy their notes in a secure manner at the conclusion of the appraisal. This requirement ensures that the attribution of detailed information to individuals in the organization cannot lead to inappropriate consequences following the appraisal.

As team members examine data sources, they record the types of objective evidence (e.g., referencing documents, presentations, instruments, and interviewee comments) as well as why or how the objective evidence meets the intent of the model practice.

Notes can be recorded for items that have significant positive or negative impact on the enactment of processes within the organizational units, even if they are not directly related to model practices. These items may ultimately be reflected in nonmodel findings reported to the organizational unit.

Table 37 summarizes this activity.

Table 37: Document Objective Evidence: Take/Review/Tag Interview Notes

Process/Activity	Required Practices
2.3 Document Objective Evidence	
2.3.1 Take/Review/Tag Interview Notes	The appraisal team shall • record notes obtained from objective evidence data-gathering sessions • relate notes to corresponding practices in the appraisal reference model

2.3.2 Record Presence/Absence of Objective Evidence

The presence or absence of appropriate objective evidence for each model practice in the scope of the appraisal is determined based on information obtained from data gathering sessions. Annotations are recorded indicating the source, relevance, and coverage of objective evidence collected. In situations where just referencing the data source would not make it obvious why the objective evidence is appropriate, a comment can be added to the annotation. Adding comments to the annotations can help avoid rehashing the rationale for accepting the objective evidence during team discussions.

Table 38 summarizes this activity.

Table 38: Document Objective Evidence: Record Presence/Absence of Objective Evidence

Process/Activity	Required Practices
2.3 Document Objective Evidence	
2.3.2 Record Presence/Absence of Objective Evidence	The appraisal team shall • for each instantiation, record the presence or absence of objective evidence collected for each reference model practice within the appraisal scope

2.3.3 Document Practice Implementation

The primary intent of this activity is to derive, from the objective evidence gathered, summary statements that describe the gap between what the objective evidence shows and what the team was looking for to support a claim that the model practice was implemented. Preliminary findings, including statements of practice implementation gaps are validated with the appraisal participants at a later time.

For any practice that is characterized as something other than Fully Implemented (refer to Section 2.4.2), there must be a statement explaining the gap between the model and what the organization does.

The appraisal team documents any significant issues impeding performance in the organization that do not necessarily map to the reference model. These may be documented as nonmodel findings in the appraisal report.

Table 39 summarizes this activity.

Table 39: Document Objective Evidence: Document Practice Implementation

Process/Activity	Required Practices
2.3 Document Objective Evidence	
2.3.3 Document Practice Implementation	The appraisal team shall • document gaps in the implemented processes relative to appraisal reference model practices

2.3.4 Review and Update the Data Collection Plan

This activity is used to continuously monitor the state of available objective evidence and to select the next tactic in the pursuit of obtaining full coverage of the reference model scope and organizational scope of the appraisal. The data collection status summarizes the differences between the objective evidence on hand and the evidence needed to support the creation of appraisal outputs such as ratings. Annotations regarding the presence and appropriateness of objective evidence allow the team to inventory the state of the knowledge base. This status then drives requirements for the collection of more data.

Table 40 summarizes this activity.

Table 40: Document Objective Evidence: Review and Update Data Collection Plan

Process/Activity	Required Practices
2.3 Document Objective Evidence	
2.3.4 Review and Update Data Collection Plan	The appraisal team shall • review the inventory of objective evidence collected and the data collection plan to determine what additional objective evidence is still needed for adequate coverage of the appraisal reference model scope • revise the data collection plan to obtain additional objective evidence for instances where available data are inadequate to judge the implementation of appraisal reference model practices • identify priorities for the upcoming data collection events and reevaluate the feasibility of the schedule in light of the current state of the objective evidence

2.4 Verify Objective Evidence

This process verifies the implementation of the organization's practices for each instantiation, describing gaps in the implementation of model practices. Each implementation of each practice

is verified so that it may be compared to the practices of the reference model. Then the team characterizes the extent to which the practices in the model are implemented. Exemplary implementations of model practices may be highlighted as strengths to be included in appraisal outputs.

Inheritance occurs when practices are performed on behalf of a subunit entity by a superunit entity within the organization. In an appraisal, a subunit entity could receive credit for having implemented a portion of the model practices when it was implemented by a superunit entity, for example, policies and procedures developed, disseminated, and administered by a superunit of the organization to serve wholly or partially the subunit entity.

This process is composed of two activities summarized in Table 41 and described below.

Table 41: Verify Objective Evidence

Process/Activity	Required Practices
2.4 Verify Objective Evidence	
2.4.1 Verify Objective Evidence	The appraisal team shall • verify the appropriateness of direct artifacts, indirect artifacts, and affirmations provided by each organizational unit for practices within the appraisal reference model scope • verify that the implementation of each model practice within the appraisal scope is supported by direct artifacts for each organizational unit within the appraisal scope and corroborated by indirect artifacts or affirmations • obtain oral affirmations corresponding to each specific and generic goal within the model scope of the appraisal for at least half (50%) of the practice instantiations for which direct artifacts are collected • generate and verify preliminary findings (i.e., statements describing strengths and/or gaps in the organizational unit's implemented practices relative to practices defined in the appraisal reference model)
2.4.2 Characterize Implementation of Model Practices	The appraisal team shall • characterize, for each instantiation, the extent to which appraisal reference model practices are implemented • aggregate practice implementation characterization values from the instantiation level to the organizational unit level

2.4.1 Verify Objective Evidence

The appraisal team establishes a clear understanding of the practices implemented in the organization. Typically, the organization provides a set of objective evidence at the beginning of the appraisal process, and the team sets out to verify the instances where those practices are implemented. One or more direct artifacts are needed to verify implementation of each model practice. Direct artifacts must be corroborated by either indirect artifacts or affirmations. The typical work products listed in the reference model provide examples of artifacts that can be used as indicators of practice implementation. Findings must be verified—that is, they must be based on corroborated objective evidence and they must be consistent with other verified findings.

Verified findings cannot be both true and mutually inconsistent; in aggregate, they constitute a set of truths about the organizational unit that must be consistent.

Only after team members have a clear understanding of the implemented practices can they compare them to the model to characterize the extent to which the organizational unit implements the practices in the model or implements acceptable practice alternatives.

Table 42 summarizes this activity.

Table 42: Verify Objective Evidence: Verify Objective Evidence

Process/Activity	Required Practices
2.4 Verify Objective Evidence	
2.4.1 Verify Objective Evidence	The appraisal team shall • verify the appropriateness of direct artifacts, indirect artifacts, and affirmations provided by each organizational unit for practices within the appraisal reference model scope • verify that the implementation of each model practice within the appraisal scope is supported by direct artifacts for each organizational unit within the appraisal scope and corroborated by indirect artifacts or affirmations • obtain oral affirmations corresponding to each specific and generic goal within the model scope of the appraisal for at least half (50%) of the practice instantiations for which direct artifacts are collected • generate and verify preliminary findings (i.e., statements describing strengths and/or gaps in the organizational unit's implemented practices relative to practices defined in the appraisal reference model)

2.4.2 Characterize Implementation of Model Practices

Once a critical mass of evidence on practice implementation has been verified, the team (or mini-team) turns to characterizing the implementation of model practices. For each practice in the model included in the selected scope, and each instance of expected use, the team documents a characterization of the extent to which the model practice (or an acceptable alternative) has been implemented. These instantiation-level characterizations are then aggregated to the organizational unit level.

Characterizations of practice implementation are used as a means to focus appraisal team effort on areas where professional judgment is needed and to aid in reaching team consensus on the extent to which practices are implemented.

Table 43 summarizes rules for characterizing instantiation-level implementations of practices. Consensus of at least a subset of appraisal team members (e.g., mini-teams, if used) is necessary for practice instantiation-level characterizations.

A weakness is defined in the glossary as "the ineffective, or lack of, implementation of one or more CERT-RMM model practices." There is no need to record a weakness when documenting objective evidence if the weakness has no impact on the goal. If the appraisal team identifies a

process improvement suggestion while characterizing the practice implementations, the suggested improvement should be recorded as a note rather than a weakness.

Table 43: Rules for Characterizing Instantiation-Level Implementations of Practices

Label	Meaning (all criteria required for each label)
Fully Implemented (FI)	• One or more direct artifacts are present and judged to be adequate. • At least one indirect artifact and/or affirmation exists to confirm the implementation. • No weaknesses are noted.
Largely Implemented (LI)	• One or more direct artifacts are present and judged to be adequate. • At least one indirect artifact and/or affirmation exists to confirm the implementation. • One or more weaknesses are noted.
Partially Implemented (PI)	• Direct artifacts are absent or judged to be inadequate. • One or more indirect artifacts or affirmations suggest that some aspects of the practice are implemented. • One or more weaknesses are noted. OR • One or more direct artifacts are present and judged to be adequate. • No other evidence (indirect artifacts, affirmations) support the direct artifact(s). • One or more weaknesses are noted.
Not Implemented (NI)	• Direct artifacts are absent or judged to be inadequate. • No other evidence (indirect artifacts, affirmation) supports the practice implementation. • One or more weaknesses are noted.
Not Yet (NY)	• The organizational unit has not yet reached the stage in the life cycle of the PA to have implemented the practice.

Table 44 summarizes rules for aggregating instantiation-level characterizations to derive organizational unit-level characterizations. Consensus of all members of the appraisal team is necessary for organizational unit-level characterizations.

These rules apply to all organizational units within the appraisal scope for which implementations have been characterized in accordance with the table above.

The column labeled “Instantiations” is the input condition—the practice implementation characterizations for the set of sampled practice instantiations from appropriate organizational units. The column labeled “Outcome” is the resulting aggregated practice implementation characterization at the appropriate organizational unit level.

Table 44: Rules for Aggregating Instantiation-Level Characterizations

Instantiations	Outcome	Remarks
All FI or NY, with at least one FI	FI	All instantiations are characterized FI or NY, with at least one FI.
All LI or FI or NY, with at least one LI	LI	All instantiations are characterized LI or FI or NY, with at least one LI.
At least one LI or FI and at least one PI or NI	LI or PI	There is at least one instantiation that is characterized as LI or FI and at least one instantiation that is characterized as PI or NI. Team judgment is applied to choose LI or PI based on whether the weaknesses, in aggregate, have a significant negative impact on goal achievement.
All PI or NI or NY, with at least one PI	PI	All instantiations are characterized PI or NI or NY, with at least one PI.
All NI or NY, with at least one NY	NI	All instantiations are characterized NI or NY, with at least one NI.
All NY	NY	All instantiations are characterized NY. There are no organizational units that have reached the stage to have implemented the practice.

The characterization of reference model practice implementation begins as soon as sufficient data are available. It is not necessary that data for every instantiation be available before the implementation of any given practice can be characterized at the instantiation level. Each instance of practice enactment is characterized using the instantiation-level characterization scheme.

The characterization of practice implementation for the organizational unit is carried out using the aggregation rules summarized in the table above. These rules provide a basis for identifying the areas where professional judgment is required, and they simplify the areas where the data are unanimous.

Table 45 summarizes this activity.

Table 45: Verify Objective Evidence: Characterize Implementation of Model Practices

Process/Activity	Required Practices
2.4 Verify Objective Evidence	
2.4.2 Characterize Implementation of Model Practices	The appraisal team shall • characterize, for each instantiation, the extent to which appraisal reference model practices are implemented • aggregate practice implementation characterization values from the instantiation level to the organizational unit level

2.5 Validate Preliminary Findings

The purpose of this process is to validate preliminary findings, including gaps in practice implementation, with members of the organizational unit. Exemplary implementations of model practices may be highlighted as strengths to be included in appraisal outputs.

This process is composed of one activity summarized in Table 46 and described below.

Table 46: Validate Preliminary Findings

Process/Activity	Required Practices
2.5 Validate Preliminary Findings	
2.5.1 Validate Preliminary Findings	The appraisal team shall • validate preliminary findings with members of the appropriate organizational unit

2.5.1 Validate Preliminary Findings

To prepare for validating the verified information, the appraisal team generates preliminary findings that summarize the practice implementation gaps. The preliminary findings are written in reference to a single model practice and are abstracted to the level of the appropriate organizational unit. The statements should not reference a specific individual, department, line of business, or other identifiable organizational unit.

This validation of preliminary findings is still primarily a data collection activity, and the intent is to validate the appraisal team's understanding of the processes implemented within the organizational unit. Feedback from participants may result in modifications to the appraisal team's inventory of objective evidence. The results of the validation activity are considered in the formulation of final findings. These latter activities cannot commence until after the validation activity has occurred. The rules of confidentiality and the expected use of appraisal data must be communicated to participants in each validation activity.

Table 47 summarizes this activity.

Table 47: Validate Preliminary Findings: Validate Preliminary Findings

Process/Activity	Required Practices
2.5 Validate Preliminary Findings	
2.5.1 Validate Preliminary Findings	The appraisal team shall • validate preliminary findings with members of the appropriate organizational unit

2.6 Generate Appraisal Results

Generating appraisal results involves rating goal satisfaction based on the extent of practice implementation throughout the organizational scope of the appraisal. The extent of practice implementation is judged based on validated data (e.g., direct, indirect, and affirmation objective evidence) collected from the entire representative sample of the organizational units. The rating of capability levels is driven by the goal satisfaction ratings. The judgment of goal satisfaction is

based on and traceable to the extent of the implementation of practices associated with that goal (or alternative practices contributing equivalently to goal satisfaction).

Success in this activity is driven by team members' ability to limit their focus to the data that support the judgments and to avoid issues that threaten their ability to be objective. This activity can create a great deal of stress for team members under pressure to help their organization do well. The appraisal team leader must skillfully facilitate this activity when external pressures exist.

This process is composed of four activities summarized in Table 48 and described below.

Table 48: Generate Appraisal Results

Process/Activity	Required Practices
2.6 Generate Appraisal Results	
2.6.1 Derive Findings and Rate Goal	The appraisal team shall • derive final findings using preliminary findings statements, feedback from validation activities, and any additional objective evidence collected during the validation activities • rate each specific goal and generic goal within the reference model scope of the appraisal, based on the practice implementation characterizations at the appropriate organizational unit level as well as the aggregation of weaknesses associated with that goal • obtain appraisal team consensus on the findings statements and ratings generated for the organizational unit level
2.6.2 Determine Process Area Capability Level	The appraisal team shall • rate the capability levels for each PA within the scope of the appraisal, based on the highest level and all levels below for which its specific goals and the generic goals within the appraisal scope have been satisfied (if this rating option was selected during planning). • rate a process area as Not Rated if any goals for the PA are rated Not Rated; a capability level will not be assigned. • designate any process area outside the appraisal scope as "not applicable"; such a process area is not rated, and a capability level will not be assigned
2.6.3 Determine Capability Profile	The appraisal team shall • generate a capability profile depicting the capability level attained for each PA within the scope of the appraisal, if this rating option was selected during planning
2.6.4 Document Appraisal Results	The appraisal team shall • document the final findings • document the capability rating outcome(s) • document the ADS

2.6.1 Derive Findings and Rate Goals

The judgments made about goal satisfaction, as well as the extent of implementation of associated practices, are driven by the findings that were documented by the appraisal team and validated by appraisal participants.

When performing goal ratings, the team judges whether or not these gaps in the implementation of practices (in aggregate) threaten the organizational unit's ability to satisfy the goals associated with the practices. When deriving final findings, the aim is to create goal-level statements that summarize the gaps in practice implementation. These statements must be abstracted to the level of the appropriate organizational unit and cannot focus on individual subunits or other increments.

A goal must be rated *Not Rated* if there are any associated practices that are not characterized at the appropriate organizational unit level or that are characterized as *Not Yet* at the appropriate organizational unit level.

A goal is rated *Not Rated* if the associated set of objective evidence does not meet the defined criteria for adequate data coverage.

The goal is rated *Satisfied* if and only if both of the following conditions are met:

- All associated practices are characterized at the organizational unit level as either *Largely Implemented* or *Fully Implemented*, and
- The aggregation of weaknesses associated with the goal does not have a significant negative impact on goal achievement.

For a goal to be rated as *Unsatisfied*, the team must be able to describe how the set of documented weaknesses (or a single weakness) led to this rating.

Table 49 summarizes this activity.

Table 49: Generate Appraisal Results: Derive Findings and Rate Goal

Process/Activity	Required Practices
2.6 Generate Appraisal Results	
2.6.1 Derive Findings and Rate Goal	The appraisal team shall • derive final findings using preliminary findings statements, feedback from validation activities, and any additional objective evidence collected during the validation activities • rate each specific goal and generic goal within the reference model scope of the appraisal, based on the practice implementation characterizations at the appropriate organizational unit level as well as the aggregation of weaknesses associated with that goal • obtain appraisal team consensus on the findings statements and ratings generated for the organizational unit level

2.6.2 Determine Process Area Capability Level

CERT-RMM has no staged representation; therefore an expression of organizational maturity is not possible. However, because CERT-RMM is a continuous representation, capability level ratings for each PA are permitted. Capability level ratings can be used as an expression of the degree of process institutionalization, and the team may make rating judgments about each PA (and associated capability level) within the scope of the appraisal. Assigning capability level ratings is an optional activity, selected at the discretion of the appraisal sponsor and documented in the appraisal input. PA satisfaction is a direct function of goal satisfaction. A PA is rated as

Satisfied if every goal contained in the PA is rated as *Satisfied*. A PA is rated as *Unsatisfied* if any goal is rated as *Unsatisfied*. Table 50 summarizes the capability level ratings.

Table 50: Capability Level Ratings

Capability Level	Process Areas
0	One or more specific goals is rated Unsatisfied.
1	Generic goal for Capability Level 1 is rated Satisfied. All specific goals are rated Satisfied.
2	Generic goals for Capability Levels 1 and 2 are rated Satisfied. All specific goals are rated Satisfied.
3	Generic goals for Capability Levels 1, 2, and 3 are rated Satisfied. All specific goals are rated Satisfied.

PA ratings need not be reported to appraisal participants if the sponsor does not wish to disclose these results. However, a documented output from this rating activity, if it is performed, is a required component in the appraisal record as well as in the ADS. See Appendix B for a sample ADS. Table 51 summarizes this activity.

Table 51: Generate Appraisal Results: Determine Process Area Capability Level

Process/Activity	Required Practices
2.6 Generate Appraisal Results	
2.6.2 Determine Process Area Capability Level	The appraisal team shall • rate the capability levels for each PA within the scope of the appraisal, based on the highest level and all levels below for which its specific goals and the generic goals within the appraisal scope have been satisfied (if this rating option was selected during planning). • rate a process area as Not Rated if any goals for the PA are rated Not Rated; a capability level will not be assigned. • designate any process area outside the appraisal scope as “not applicable”; such a process area is not rated, and a capability level will not be assigned

2.6.3 Determine Capability Profile

When using CERT-RMM as the appraisal reference model, the team may determine a capability profile that graphically depicts the capability level ratings assigned to each PA within the scope of the appraisal. The generation of a capability profile is an optional activity, selected at the discretion of the appraisal sponsor and documented in the appraisal plan.

A simple bar chart can be used for this display. Each PA is represented in a single bar along the horizontal axis, and the vertical axis represents the capability level dimension. The height of each bar represents the capability level of the PA. Capability levels take only the values 0, 1, 2, or 3. Intermediate values (e.g., 1.7) are not defined for this appraisal outcome, and any embellishment of the capability profile with such values is outside the boundaries of the CERT-RMM class A capability appraisal method.

Table 52 summarizes this activity.

Table 52: Generate Appraisal Results: Determine Capability Profile

Process/Activity	Required Practices
2.6 Generate Appraisal Results	
2.6.3 Determine Capability Profile	The appraisal team shall • generate a capability profile depicting the capability level attained for each PA within the scope of the appraisal, if this rating option was selected during planning

2.6.4 Document Appraisal Results

The results of the appraisal must be documented for reporting. Oral reports of the rating outcomes or oral explanations of implementation gaps discovered by the team are not adequate to communicate appraisal results.

This activity is focused on collecting and documenting the results of prior activities related to the generation of findings and ratings. Depending on the planned recipients of the results, multiple forms of the results may be needed. Certain data may not be appropriate for all audiences, or the style or language of the results may need to be adjusted to best fit the needs of the recipients.

Table 53 summarizes this activity.

Table 53: Generate Appraisal Results: Document Appraisal Results

Process/Activity	Required Practices
2.6 Generate Appraisal Results	
2.6.4 Document Appraisal Results	The appraisal team shall • document the final findings • document the capability rating outcome(s) • document the ADS

3 Report Results

The Reporting Appraisal Results phase (see Table 54) is composed of two processes: Deliver Appraisal Results and Package and Archive Appraisal Assets. Each of these processes has additional tasks and activities explained in subsequent sections.

Table 54: Report Results

Process	Activity
3.1 Deliver Appraisal Results	3.1.1 Deliver Final Findings
	3.1.2 Conduct Executive Session(s)
	3.1.3 Plan for Next Steps
3.2 Package and Archive Appraisal Assets	3.2.1 Collect Lessons Learned
	3.2.2 Generate Appraisal Record
	3.2.3 Provide Appraisal Data to SEI CERT-RMM Steward
	3.2.4 Archive and/or Dispose of Appraisal Assets

3.1 Deliver Appraisal Results

The purpose of this process is to provide credible appraisal results that can be used to guide improvement actions. Appraisal results represent the strengths and weaknesses of the processes in use at the time. Results include ratings (if planned for) that accurately reflect the capability level of the processes as appraised. The appraisal results are intended to support decision making and should be delivered in a way that promotes appropriate actions.

This process is composed of three activities summarized in Table 55 and described below.

Table 55: Deliver Appraisal Results

Process/Activity	Required Practices
3.1 Deliver Appraisal Results	
3.1.1 Deliver Final Findings	The appraisal team leader or designee shall • provide appraisal final findings, signed by the appraisal team leader and all appraisal team members, to the appraisal sponsor • provide an ADS to the appraisal sponsor summarizing the appraisal results and conditions under which the appraisal was performed. The ADS must be signed by the appraisal team leader and appraisal sponsor.
3.1.2 Conduct Executive Session(s)	None
3.1.3 Plan for Next Steps	None

3.1.1 Deliver Final Findings

The final findings contain a summary of the strengths and weaknesses for each PA within the appraisal scope, as well as additional information that provides context for the findings. The generation of the findings is addressed in Activity 2.6.1, Derive Findings and Rate Goals; this activity relates to the delivery of these findings to the appraisal sponsor and appraised

organization. These findings may be in a summarized form, with the detailed findings provided as backup information, and are often presented using slides in a meeting room or auditorium.

In addition to the final findings, a draft ADS summarizing the results of the appraisal is provided to the appraisal sponsor. Confidentiality and nonattribution principles apply to statements made in the presentation of final findings.

Table 56 summarizes this activity.

Table 56: Deliver Appraisal Results: Deliver Final Findings

Process/Activity	Required Practices
3.1 Deliver Appraisal Results	
3.1.1 Deliver Final Findings	The appraisal team leader or designee shall • provide appraisal final findings, signed by the appraisal team leader and all appraisal team members, to the appraisal sponsor • provide an ADS to the appraisal sponsor summarizing the appraisal results and conditions under which the appraisal was performed. The ADS must be signed by the appraisal team leader and appraisal sponsor.

3.1.2 Conduct Executive Session(s)

The executive session is an optional activity that may be performed at the discretion of the appraisal sponsor or senior site manager. The executive session provides the appraisal sponsor, senior organizational units manager(s), and invited staff a private opportunity to (a) discuss with the appraisal team leader any issues with the appraisal, (b) obtain clarification of the appraisal results, (c) confirm understanding of the process issues, and (d) provide guidance regarding focus, timing, and priorities of the recommendations report and follow-on activities. If an executive session is conducted, the confidentiality and nonattribution of data sources must be maintained.

Table 57 summarizes this activity.

Table 57: Deliver Appraisal Results: Conduct Executive Session(s)

Process/Activity	Required Practices
3.1 Deliver Appraisal Results	
3.1.2 Conduct Executive Session(s)	None

3.1.3 Plan for Next Steps

Following the delivery of the appraisal results, a plan for follow-on activities is determined. The planned follow-on activities are typically defined in the appraisal plan, reflecting sponsor requests for additional appraisal tasks and products necessary to meet appraisal objectives or for a commitment to take action on the appraisal results. Follow-on activities may include the following:

- development of a final report
- development of a recommendations report or briefing
- generation or update of a process improvement plan

Table 58 summarizes this activity.

Table 58: Deliver Appraisal Results: Plan for Next Steps

Process/Activity	Required Practices
3.1 Deliver Appraisal Results	
3.1.3 Plan for Next Steps	None

3.2 Package and Archive Appraisal Assets

The purpose of this process is to preserve important data and records from the appraisal and dispose of sensitive materials in an appropriate manner.

This process is composed of four activities summarized in Table 59 and described below.

Table 59: Package and Archive Appraisal Assets

Process/Activity	Required Practices
3.2 Package and Archive Appraisal Assets	
3.2.1 Collect Lessons Learned	None
3.2.2 Generate Appraisal Record	The appraisal team leader or designee shall • collect and record baseline appraisal data that become part of the permanent records provided to appraisal stakeholders • document the satisfaction of all CERT-RMM class A capability appraisal requirements • generate the appraisal record from baselined planning and execution data collected throughout the appraisal • place appraisal records and other appraisal data under appropriate confidentiality, integrity, availability, and configuration controls • deliver the appraisal record to the appraisal sponsor
3.2.3 Provide Appraisal Data to SEI CERT-RMM Steward	The appraisal team leader or designee shall • submit the completed appraisal data package as required by the SEI CERT-RMM Steward
3.2.4 Archive and/or Dispose of Appraisal Artifacts	The appraisal team leader or designee shall • archive or dispose of key artifacts collected by the appraisal team • return objective evidence provided by the organizational unit

3.2.1 Collect Lessons Learned

As one of the final activities in wrapping up an appraisal, teams typically record lessons learned from their experience. The purpose of these lessons learned is to document what went right, what went wrong, and any suggestions or recommendations for improving the method or its execution.

The collection of lessons learned is a recommended activity for the improvement of future appraisals, but it is not a method requirement.

Table 60 summarizes this activity.

Table 60: Package and Archive Appraisal Assets: Collect Lessons Learned

Process/Activity	Required Practices
3.2 Package and Archive Appraisal Assets	
3.2.1 Collect Lessons Learned	None

3.2.2 Generate Appraisal Record

Appraisal data collected throughout the appraisal is aggregated and summarized into a permanent record documenting the appraisal conduct and results. This collection of data is referred to as the appraisal record and is delivered to the appraisal sponsor for retention.

Appraisal data must comply with rules for nonattribution; confidentiality; protection of proprietary information; and applicable laws, regulations, or standards (e.g., acquisition regulations or security classification). Recipients are expected to place the appropriate limitations on the access and use of the provided appraisal data.

Table 61 summarizes this activity.

Table 61: Package and Archive Appraisal Assets: Generate Appraisal Record

Process/Activity	Required Practices
3.2 Package and Archive Appraisal Assets	
3.2.2 Generate Appraisal Record	The appraisal team leader or designee shall • collect and record baseline appraisal data that become part of the permanent records provided to appraisal stakeholders • document the satisfaction of all CERT-RMM class A capability appraisal requirements • generate the appraisal record from baselined planning and execution data collected throughout the appraisal • place appraisal records and other appraisal data under appropriate confidentiality, integrity, availability, and configuration controls • deliver the appraisal record to the appraisal sponsor

3.2.3 Provide Appraisal Data to SEI CERT-RMM Steward

Appraisal data required by the SEI CERT-RMM Steward are collected and reported. These data include a subset of the contents of the appraisal record, as well other data used by the Steward to aggregate and analyze appraisal performance data for reporting to the community and monitoring the quality of performed appraisals.

Table 62 summarizes this activity.

Table 62: Package and Archive Appraisal Assets: Provide Appraisal Data to SEI CERT-RMM Steward

Process/Activity	Required Practices
3.2 Package and Archive Appraisal Assets	
3.2.3 Provide Appraisal Data to SEI CERT-RMM Steward	The appraisal team leader or designee shall • submit the completed appraisal data package as required by the SEI CERT-RMM Steward

3.2.4 Archive and/or Dispose of Appraisal Assets

After the various reports are delivered to the appropriate stakeholders and the appraisal artifacts (e.g., work products, presentations, documents, etc.) have been documented, baselined, and placed under appropriate confidentiality, integrity, availability, and configuration controls, the appraisal team leader is responsible for properly archiving and/or disposing of the appraisal data, in accordance with agreements made with the sponsor and documented in the appraisal plan. The team librarian (if one is used) ensures that all documentation and objective evidence provided by the organizational units is returned or disposed of properly. Any remaining team artifacts or notes are disposed of properly.

Table 63 summarizes this activity.

Table 63: Package and Archive Appraisal Assets: Archive and/or Dispose of Appraisal Artifacts

Process/Activity	Required Practices
3.2 Package and Archive Appraisal Assets	
3.2.4 Archive and/or Dispose of Appraisal Artifacts	The appraisal team leader or designee shall • archive or dispose of key artifacts collected by the appraisal team • return objective evidence provided by the organizational unit

Appendix A SCAMPI MDD V1.2 Traceability Matrix

To maintain fidelity and consistency with SCAMPI MDD V1.2, the phases and processes in the CERT-RMM CAM V1.1 share its nomenclature. Some activities in the SCAMPI MDD V1.2 have been eliminated or modified significantly in this report. The tables in this appendix are provided to maintain traceability between the SCAMPI MDD V1.2 phases and processes and the CERT-RMM CAM phases and processes.

Table 64: SCAMPI MDD V1.2 Traceability Matrix, Phase 1: Plan and Prepare for Appraisal

Phase	Process	SCAMPI MDD V1.2 Activities	CERT-RMM CAM V1.1 Activities
1. Plan and Prepare for Appraisal	1.1 Analyze Requirements	1.1.1 Determine Appraisal Objectives 1.1.2 Determine Appraisal Constraints 1.1.3 Determine Appraisal Scope 1.1.4 Determine Outputs 1.1.5 Obtain Commitments to Appraisal Input	1.1.1 Determine Appraisal Objectives 1.1.2 Determine Appraisal Constraints 1.1.3 Determine Appraisal Scope 1.1.4 Determine Outputs 1.1.5 Obtain Commitments to Appraisal Input
	1.2 Develop Appraisal Plan	1.2.1 Tailor Method 1.2.2 Identify Needed Resources 1.2.3 Determine Cost and Schedule 1.2.4 Plan and Manage Logistics 1.2.5 Document and Manage Risks 1.2.6 Obtain Commitment to Appraisal Plan	1.2.1 Tailor Method 1.2.2 Identify Needed Resources 1.2.3 Determine Cost and Schedule 1.2.4 Plan and Manage Logistics 1.2.5 Document and Manage Risks 1.2.6 Obtain Commitment to Appraisal Plan
	1.3 Select and Prepare Team	1.3.1 Identify Appraisal Team Leader 1.3.2 Select Team Members 1.3.3 Prepare Team	1.3.1 Identify Appraisal Team Leader 1.3.2 Select Team Members 1.3.3 Prepare Team
	1.4 Obtain and Inventory Initial Objective Evidence	1.4.1 Obtain Initial Objective Evidence 1.4.2 Inventory Objective Evidence	1.4.1 Obtain Initial Objective Evidence 1.4.2 Inventory Objective Evidence
	1.5 Prepare for Appraisal Conduct	1.5.1 Perform Readiness Review 1.5.2 Prepare Data Collection Plan 1.5.3 Replan Data Collection (if needed)	1.5.1 Perform Readiness Review 1.5.2 Prepare Data Collection Plan 1.5.3 Replan Data Collection (if needed)

Table 65: SCAMPI MDD V1.2 Traceability Matrix, Phase 2: Conduct Appraisal

Phase	Process	SCAMPI MDD V1.2 Activities	CERT-RMM CAM V1.1 Activities
2. Conduct Appraisal	2.1 Prepare Participants	2.1.1 Conduct Participant Briefing	2.1.1 Conduct Participant Briefing
	2.2 Examine Objective Evidence	2.2.1 Examine Objective Evidence from Documents 2.2.2 Examine Objective Evidence from Interviews	2.2.1 Examine Objective Evidence
	2.3 Document Objective Evidence	2.3.1 Take/Review/Tag Notes 2.3.2 Record Presence/Absence of Objective Evidence 2.3.3 Document Practice Implementation 2.3.4 Review and Update the Data Collection Plan	2.3.1 Take/Review/Tag Notes 2.3.2 Record Presence/Absence of Objective Evidence 2.3.3 Document Practice Implementation 2.3.4 Review and Update the Data Collection Plan
	2.4 Verify Objective Evidence	2.4.1 Verify Objective Evidence 2.4.2 Characterize Implementation of Model Practices	2.4.1 Verify Objective Evidence 2.4.2 Characterize Implementation of Model Practices
	2.5 Validate Preliminary Findings	2.5.1 Validate Preliminary Findings	2.5.1 Validate Preliminary Findings
	2.6 Generate Appraisal Results	2.6.1 Derive Findings and Rate Goals 2.6.2a Determine Process Area Capability Level 2.6.2b Determine Satisfaction of Process Areas 2.6.3a Determine Capability Profile 2.6.3b Determine Maturity Level 2.6.4 Document Appraisal Results	2.6.1 Derive Findings and Rate Goals 2.6.2 Determine Process Area Capability Level 2.6.3 Determine Capability Profile 2.6.4 Document Appraisal Results

Table 66: SCAMPI MDD V1.2 Traceability Matrix, Phase 3: Report Results

Phase	Process	SCAMPI MDD V1.2 Activities	CERT-RMM CAM V1.1 Activities
3. Report Results	3.1 Deliver Appraisal Results	3.1.1 Deliver Final Findings 3.1.2 Conduct Executive Session(s) 3.1.3 Plan for Next Steps	3.1.1 Deliver Final Findings 3.1.2 Conduct Executive Session(s) 3.1.3 Plan for Next Steps
	3.2 Package and Archive Appraisal Assets	3.2.1 Collect Lessons Learned 3.2.2 Generate Appraisal Record 3.2.3 Provide Appraisal Feedback to CMMI Steward 3.2.4 Archive and/or Dispose of Key Artifacts	3.2.1 Collect Lessons Learned 3.2.2 Generate Appraisal Record 3.2.3 Provide Appraisal Feedback to CERT-RMM Steward 3.2.4 Archive and/or Dispose of Key Artifacts

Appendix B Example Appraisal Disclosure Statement (ADS)

This is an example of an appraisal disclosure statement.

CERT Resilience Management Model Class A Appraisal Disclosure Statement for _____

August 2010

Document Updates

Changes to any of the information contained in this document should be handled via appropriate entries in the document Revision History table below.

Revision History

Version	Date	Summary of Changes
0.1	07/29/2010	Draft version for review with appraisal sponsor

Introduction

This document is the CERT® Resilience Management Model (CERT®-RMM) class A Appraisal Disclosure Statement to be performed for _____ in the August 2010 time frame. The purpose of this document is to record the results of appraisal planning including the requirements, agreements, estimates, risks, method tailoring, and practical considerations (e.g., schedules, logistics, and contextual information about the organization) associated with the appraisal. This document is a required appraisal method artifact that must be reviewed and approved by the appraisal team leader and the appraisal sponsor.

Appraisal Purpose

Business Objectives

Appraisal Objectives

Key Appraisal Participant Information

Appraisal Sponsor

Name	
Title	
Organizational Affiliation	
Relationship to the Organizational Unit Being Appraised	
Mailing Address	
Phone	
Email	

Appraisal Team Leader

Name	
Appraisal Leadership Credentials	
Title	
Organizational Affiliation	
Mailing Address	
Phone	
Email	

Appraisal Team Members Identification

Name	Organizational Affiliation	Reporting Relationships	Contact Information

Qualifications and Responsibilities

Name	Introduction to CERT Resilience Management Model	Specific Appraisal Responsibilities
		Team Leader
		Team Member
		Team Member
		Team Member

Rationale for Selecting Team Members

Organizational Unit Appraisal Participants and Support Staff

Name	Organizational Affiliation	Specific Appraisal Responsibilities
		Site Coordinator
		Evidence preparation
		Interviewee
		Interviewee

Appraisal Scope Specification

Organizational Unit

Groups or Functions Specifically Excluded from the Organizational Unit and the Justification for Their Exclusion

Organizational Scope (Participating Organizational Units)

Organizational unit 1

Subunit name:

Subunit type:

Process areas for which objective evidence will be collected and analyzed:

Placement within organization unit:

Geographical location(s) of organizational unit:

Rationale for Selecting These Subunits in the Organizational Unit

Model to be Used

CERT-RMM Model Scope

Process Context Information

Organizational Unit Size and Demographics

Organizational Unit Domain(s) Characterization

High-Priority Characteristics for Products and Services

Key Appraisal Parameters

Appraisal Usage Mode

_____ Internal Process Improvement

_____ Source Selection

_____ Process Monitoring

Planned Tailoring and Associated Tradeoffs

Appraisal Outputs

This section identifies artifacts and other appraisal outputs to be produced.

Will Be Generated	Output	Comments
	Increment-specific findings	
	Project-specific findings	
	OU-level findings	
	Practice characterizations instantiation level	
	Practice characterizations OU level	
	Recommendations on how to address weaknesses	
	Final findings presentation slides	
	Final appraisal report	
	Appraisal disclosure statement	
	Appraisal record	
	Appraisal feedback forms (SAS)	
	Appraisal data package	
	Process improvement action plan	

Appraisal Results Delivery Method

A final findings presentation, containing designated appraisal results, will be made to the appraisal sponsor and other invitees of the sponsor's choosing on the final day of the on-site activities and repeated virtually a few weeks later for a larger audience.

Appraisal Constraints

Key Resources

Staffing

An appraisal is an intense activity requiring the full-time concentration of all identified appraisal team members during the on-site period. Personnel assigned to be a member of the appraisal team must be available for 100 percent of their time during the appraisal on-site. If an individual fails to be available as required, the team leader may decide to remove the individual from the team.

Funding

Funding has been established to cover all of the planned appraisal preparation, conduct, wrap-up activities, and related travel. This funding has been provided for all of the personnel supporting the appraisal.

The appraisal will be conducted in accordance with any contractual provisions relating to the price/cost of the appraisal activities. The price/cost was determined in good faith based on information contained in this document; however, if the actual circumstances or readiness of the organization to proceed with the appraisal differ from those documented herein to the extent that the appraisal cannot be completed within the agreed-to cost and schedule, the team leader will confer with the appraisal sponsor to determine the appropriate course of action. Possible actions are (1) terminate the appraisal, (2) replan the appraisal scope to fit within the original cost and schedule, or (3) continue the appraisal under the original scope but with renegotiated cost and schedule.

Duration

The duration of the appraisal will be driven primarily by the scope of the appraisal and secondarily by team size. Use of mini-teams is not planned in this appraisal; all activities associated with characterizing practice implementations will be performed with consensus by the entire appraisal team.

Tools

Each appraisal team member will require exclusive use of a computer with appropriate software installed (Microsoft Word, PowerPoint, Excel), access to a computer display projection device and screen, and printer/copying facilities during the duration of the appraisal on-site. External team members will bring their own laptop computers and will require appropriate authorizations to bring their personal equipment in/out of the facility. If authorization to bring personal equipment in/out of the facility cannot be granted for any reason, the organization must provide the affected external team members with exclusive use of a computer during the appraisal onsite activities.

The appraisal team members will need to share and exchange data during the appraisal on-site activities and plan to use portable USB drives for this purpose. The team must have authorization to bring such storage media in/out of the facility and to use such media for the purpose of transferring files to one another.

Facilities

Appraisal team members who are not from the local organization will require access to the facility for the duration of the appraisal. The appraisal team will also require exclusive use of a room or other equivalent facility large enough to accommodate the entire team and their equipment, room to spread out documents being reviewed, and room to interview organization personnel. Since the team will be generating sensitive information during the course of the appraisal, this facility must be capable of being physically secured to prevent unauthorized access to appraisal materials. The facility chosen for this purpose must have sufficient power, lighting, and networking capabilities (if required to access organizational assets for the appraisal). The room must also be equipped with a computer projection device and display screen to enable the team to effectively review and collaborate on appraisal documents.

The appraisal team will present briefings to the organization during the course of the appraisal and will require appropriate conference rooms adequate to hold the expected number of attendees. These briefings, at a minimum, will consist of the final findings presentation.

Required class A team training will be conducted. A computer projector will be required to enable projection of the training material.

Schedule Constraints

Appraisal Scope Constraints

This is a continuous representation appraisal, and only those process areas identified in the CERT-RMM model scope will be examined.

No organizational entities are excluded from this appraisal. The practices to be examined in this appraisal are applicable to the entire organizational unit as defined in the “Organizational Unit” section.

Information Management and Ownership

Ownership of Appraisal Results

Appraisal Output	Owner	Restrictions on use
Appraisal plan	Appraisal sponsor	
All versions of the PIID workbook containing organizational data	Appraisal sponsor	No copies of the PIID workbook shall be kept by any appraisal team member without permission from the appraisal sponsor.
Final findings presentation materials (MS PowerPoint file)	Appraisal Sponsor	No copies of the final findings presentation shall be kept by any appraisal team member without permission from the appraisal sponsor.

Controls Resulting from Confidentiality Agreement(s)

All appraisal team members and appraisal participants (e.g., interviewees) shall sign a confidentiality and nonattribution agreement that is specific to the appraisal activities.

Nonattribution Provisions

All findings will be written without attribution to the individuals providing the information in the interviews and without attribution to specific organizational units.

Other

Additional Information Needed

Anticipated Follow-on Activities

Activities, Resources, and Schedule

A readiness review will be held as a teleconference on _____. The appraisal onsite activities will be conducted starting on _____ and ending on _____. Because of the dynamic nature of the detailed schedule for on-site activities, that schedule will be maintained separately from this plan.

Appraisal Logistics

The site coordinator is responsible for

- reserving required conference and interview rooms
- providing overhead projection capability
- addressing issues related to site logistics such as access to a network printer
- providing the appraisal team with required office supplies
- obtaining printouts and copies of documents if needed by the appraisal team
- arranging for the interview sessions and supporting attendance

Risk Management

This section addresses the risks considered the most significant to the success of the appraisal.

Identified Risks

Risks associated with appraisal execution have been identified and are listed below. Mitigation and/or contingency plans are also provided. Risk status will be tracked on a regular basis.

No.	Description	Probability & impact	Impact details	Mitigation	Responsibility
1	Appraisal team leader (ATL) is not available as planned	P: Low I: High	-Schedule impact due to bringing the new ATL up to speed on the appraisal	-Identify backup for ATL -Monitor circumstances that would impact ATL availability	ATL and sponsor
2	Appraisal team member (ATM) is not available as planned	P: Low I: Medium	-Schedule impact due to bringing the new ATM up to speed on the appraisal or accomplishing the appraisal with smaller team	-Expanded number of ATMs allows appraisal to be completed if one ATM is unavailable -Replan the remaining appraisal activities if risk is realized	ATL and sponsor
3	Interviewees are unavailable	P: Low I: Low	-Unable to conduct interviews	-Attempt to schedule alternate interviewee	ATL and sponsor
4	Site is inaccessible during planned on-site period	P: Low I: High	-Appraisal could not be completed as scheduled unless alternative site was made available with necessary access and infrastructure -Schedule risk	-Reschedule on-site -Conduct on-site at another facility or at a hotel meeting room (assuming that access to all evidence could be made available at the alternative location)	ATL and sponsor
5	Appraisal team is unable to reach consensus decision on a finding or characterization	P: Low I: High	-Appraisal findings depend on consensus agreement by the appraisal team. If the team is unable to reach consensus, the appraisal completion and results are at risk.	-If the appraisal team is unable to reach consensus after considerable discussion and debate, a. The team will mark the issue as "open" and proceed with other discussions. After some time has passed, the team will revisit the issue to attempt again to reach consensus. b. If a single team member is in disagreement with the remainder of the team and that team member was responsible for preparing or developing the evidence in question, then the sponsor will be consulted. With the sponsor's concurrence, the team will exclude the single member from the decision in question. c. If persistent consensus issues are encountered, the ATL and sponsor may revise the team membership during the appraisal as may be appropriate.	ATL and sponsor

Affirmations

Appraisal Team Leader (required)

As the designated CERT-RMM Capability Appraisal Method Class A Team Leader for this appraisal, I affirm that to the best of my knowledge the information in this document is accurate, does reflect my current agreement with the appraisal sponsor, and does contain the minimum information required by the CERT-RMM Capability Appraisal Method and the provisions of my authorization as a CERT-RMM Capability Appraisal Team Leader.

Appraisal Team Leader	Date

Appraisal Sponsor (required)

As the sponsor for this appraisal, I affirm that I have reviewed and do approve this Appraisal Plan document.

Appraisal Sponsor	Date

Glossary of Terms

This is an alphabetical glossary of terms for the CERT Resilience Management Model with additional terms added to support the Capability Appraisal Method (CAM) V1.1. The glossary provides definitions based on how the term is used in the context of operational resilience management. For this reason, the definitions provided may differ from those in common use.

The origin for each term is noted in brackets at the end of each definition. The notation refers to the CERT-RMM process area where the term originates or is used. For example, [AM] refers to the Access Management process area.

Terms marked with an asterisk (*) are new additions to the CERT-RMM glossary.

abuse case
See "misuse/abuse case."

access acknowledgement
A form or process that allows users to acknowledge (in writing) that they understand their access privileges and will abide by the organization's policy regarding the assignment, use, and revocation of those privileges. [AM]

access control
The administrative, technical, or physical mechanism that provides a "gate" at which identities must present proper credentials and be authenticated to pass. [AM] [KIM]

access control policy (access management policy)
An organizational policy that establishes the policies and procedures for requesting, approving, and providing access to persons, objects, and entities and establishes the guidelines for disciplinary action for violations of the policy. [AM]

Access Management (AM)
An operations process area in CERT-RMM. The purpose of Access Management is to ensure that access granted to organizational assets is commensurate with their business and resilience requirements.

access privilege
A mechanism for describing and defining an appropriate level of access to an organizational asset—information, technology, or facilities—commensurate with an identity's job responsibilities and the business and resilience requirements of the asset. [AM] [HRM]

access request
A mechanism for requesting access to an organizational asset that is submitted to and approved by owners of the asset (with sufficient justification). [AM]

acculturation
The acquisition and adoption of a process improvement mindset and culture for resilience throughout all levels of the organization. [HRM]

adaptive maintenance
Maintenance performed to adapt a facility to a different operating environment. [EC]

adequate*
The quality of being able to meet a need satisfactorily. For example, adequate resilience requirements meet the need for a protection or sustainability objective in the most efficient manner and with full consideration of the risks to the asset, business process, or service. In the case of an appraisal, "adequate" is used to determine if coverage requirements have been met. See "coverage criteria" and "sufficient coverage."

administrative control
A type of managerial control that ensures alignment to management's intentions and includes such artifacts as governance, policy, monitoring, auditing, separation of duties, and the development and implementation of service continuity plans. [KIM]

affirmation*
An oral or written statement confirming or supporting implementation, or lack of implementation, of a model specific practice or generic practice.

agreement
A legal agreement between the organization and a business partner or supplier. The agreement may be a contract, a license, or a memorandum of agreement (MOA). The agreement is legally binding. Performance measures against the agreement are typically created and documented in a service level agreement (SLA), a secondary agreement that often supports the legal agreement.

alternative practice*
A practice that is a substitute for one or more generic or specific practices that achieves an equivalent effect towards satisfying the generic or specific goal associated with model practices. [ARC V1.1]

Appraisal Disclosure Statement*
An Appraisal Disclosure Statement (ADS) is a summary statement describing the ratings generated as outputs of the appraisal as well as the conditions and constraints under which the appraisal was performed. The ADS should be used for public disclosures of capability level ratings so they can be interpreted accurately.

appraisal findings*
The results of an appraisal that identify the most important issues, problems, or opportunities for process improvement within the appraisal scope. [ARC V1.1]

appraisal objectives*
The desired outcomes of an appraisal. [ARC V1.1]

appraisal output*
All of the tangible results from an appraisal. (See related glossary term "appraisal record.")

appraisal rating*
The value assigned by an appraisal team to a CERT-RMM goal or process area or the capability level of a process area.

appraisal record*
An orderly, documented collection of information that is pertinent to the appraisal and adds to the understanding and verification of the appraisal findings and capability level ratings generated.

appraisal scope
The part of the organization that is the focus of a CERT-RMM-based appraisal of current resilience practices. The scope of an appraisal is typically, but not necessarily, the same as the scope of the improvement effort. (See related glossary terms “model scope” and “organizational scope.”)

appraisal tailoring*
Selection of options within the appraisal method for use in a specific instance. The intent of tailoring is to assist an organization in aligning application of the appraisal outcomes with its business needs and objectives. [ARC V1.1]

area of impact (organizational impact area)
Areas in which criteria are established to determine and express the potential impact of realized risk on the organization. Typical areas of impact include life and safety of employees and customers, financial, legal, and productivity. [RISK]

artifact*
A tangible form of objective evidence indicative of work being performed that is a direct or indirect result of implementing a model practice. (See related glossary terms “direct artifact” and “indirect artifact.”)

asset (organizational asset)
Something of value to the organization; typically, people, information, technology, and facilities that high-value services rely on. [ADM]

asset custodian
A person or organizational unit, internal or external to the organization, responsible for satisfying the resilience requirements of a high-value asset while it is in their care. For example, a system administrator on a server that contains the vendor database would be a custodian of that asset. [ADM] [RRM]

Asset Definition and Management (ADM)
An engineering process area in CERT-RMM. The purpose of Asset Definition and Management is to identify, document, and manage organizational assets during their life cycle to ensure sustained productivity to support organizational services.

asset disposition
The retirement of an asset from service, particularly information assets, commensurate with resilience requirements and information categorization and in accordance with any applicable rules, laws, and regulations. [KIM]

asset inventory
An inventory (or inventories) of organizational assets—people, information, technology, and facilities. [ADM]

asset-level resilience requirements
Asset-specific requirements that are set by the owners of the asset and are intended to establish the asset's protection and continuity needs with respect to its role in supporting mission assurance of a high-value service. [RRD]

asset life cycle
The phases of an asset's life from development or acquisition to deployment to disposition. [ADM]

asset owner
A person or organizational unit, internal or external to the organization, that has primary responsibility for the viability, productivity, and resilience of an organizational asset. For example, the Accounts Payable department is the owner of the vendor database. [ADM] [RRM]

asset profile
Documentation of specific information about an asset (typically an information asset) that establishes ownership, a common definition, and other characteristics of the asset, such as its value. [ADM]

assurance case
A structured set of arguments and a corresponding body of evidence demonstrating that a system satisfies specific claims with respect to its security, safety, or reliability properties. [RTSE]

attack pattern
A design pattern describing the techniques that attackers might use to break a software product. [RTSE]

attack surface
The set of ways in which an attacker can enter and potentially cause damage to a system. The larger the attack surface, the more insecure the system [http://www.cs.cmu.edu/~pratyus/as.html]. [RTSE]

availability
For an asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed. [EC] [KIM] [PM]

awareness
Focusing the attention of, creating cognizance in, and acculturating people throughout the organization to resilience issues, concerns, policies, plans, and practices. [OTA]

awareness activity
A means for implementing the awareness approaches that the organization has considered and developed to meet the specific needs of the stakeholder community. Formal awareness training sessions, newsletters, email messages, and posters and other signage are examples of awareness activities. [OTA]

awareness training
A means by which the organization can highlight important behaviors and begin the process of acculturating staff and business partners to important organizational resilience goals, objectives, and critical success factors. [OTA]

awareness training waiver
See "waiver." [OTA]

base measures
Data obtained by direct measurement. For example, the number of service continuity plans updated in the last 12 months is a base measure. [MA]

baseline configuration item
A configuration item that serves as the baseline foundation for managing the integrity of the asset as it changes over its life cycle. [TM]

business process
A series of discrete activities or tasks that contribute to the fulfillment of a service mission. (See related glossary term "service.")

business requirement
A requirement that must be met to achieve business objectives. Such requirements establish the baseline for how organizational assets are used to support business processes. [ADM]

capability level
An indicator of achievement of process capability in a process area. A capability level is achieved by visibly and verifiably implementing the required components of a process area. (See related glossary terms "required component" and "process area.")

capacity planning
The process of determining the operational demand for a technology asset over a widely variable range of operational needs. [TM]

CERT-RMM steward*
CERT, part of the Software Engineering Institute (SEI) at Carnegie Mellon University, is the steward of the RMM product suite.

change control (change management)
A continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption. [RRM] [TM] [KIM]

co-location (also collocation or colocation)
The act or result of placing or arranging together. In facilities management, collocation refers to the grouping of facilities, the effects of which must be considered in service continuity planning. [EC]

Communications (COMM)
An enterprise process area in CERT-RMM. The purpose of Communications is to develop, deploy, and manage internal and external communications to support resilience activities and processes.

communications stakeholder
A person or group that has a vested interest in being involved in or a beneficiary of the organization's resilience communications activities. [COMM]

Compliance (COMP)
An enterprise process area in CERT-RMM. The purpose of Compliance Management is to ensure awareness of and compliance with an established set of relevant internal and external guidelines, standards, practices, policies, regulations, legislation, and other obligations (such as contracts and service level agreements) related to managing operational resilience.

compliance
A process that characterizes the activities that the organization performs to identify the internal and external guidelines, standards, practices, policies, regulations, and legislation to which they are subject and to comply with these obligations in an orderly, systematic, efficient, timely, and accurate manner. [COMP]

compliance knowledgebase
A common accessible information repository for compliance data. The repository may include documentation of the compliance obligations and their owners and due dates, the results of compliance and substantive testing of controls, compliance targets and metrics, compliance reports, noncompliance reports, remediation plans, and tracking data to provide status on satisfying compliance obligations. [COMP]

compliance obligations
The internal and external guidelines, standards, practices, policies, regulations, and legislation that the organization has an obligation to comply with. [COMP]

condition
A term that collectively describes a vulnerability, an actor, a motive, and an undesirable outcome. A condition is essentially a threat that the organization must identify and analyze to determine if exploitation of the threat could result in undesirable consequences. [RISK] (See related glossary term "consequence.")

confidentiality
For an asset, the quality of being accessible only to authorized people, processes, and devices. [KIM]

configuration item
An asset or a series of related assets (typically information or technology-focused) that are placed under configuration management processes. [KIM] [TM]

configuration management
A process for managing the integrity of an information or technology asset over its lifetime. Typically includes change control processes. [KIM] [TM]

consensus*
A method of decision making that allows team members to develop a common basis of understanding and agreement concerning a decision that all team members are willing to support. [ARC V1.1]

consequence
The unwanted effect, undesirable outcome, or impact to the organization as the result of exploitation of a condition or threat. [RISK] (See related glossary term “condition.”)

constellation
In the CMMI architecture, a collection of components that are used to construct models, training materials, and appraisal materials in an area of interest (e.g., services and development).

container (information asset container)
A physical or logical location where assets are stored, transported, and processed. A container can encompass technical containers (servers, network segments, personal computers), physical containers (paper, file rooms, storage spaces, or other media such as CDs, disks, and flash drives), and people (including people who might have detailed knowledge about the information asset). [KIM]

continuity of operations
An organization’s ability to sustain assets and services in light of realized risk. Typically used interchangeably with service continuity. [RISK] [SC] (See related glossary term “Service Continuity.”)

controls
The methods, policies, and procedures—manual or automated—that are adopted by an organization to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, the promotion of administrative efficiency, and adherence to standards. [CTRL] [KIM]

Controls Management (CTRL)
An engineering process area in CERT-RMM. The purpose of Controls Management is to establish, implement, monitor, and manage an internal control system that ensures the effectiveness and efficiency of operations through mission assurance of high-value services.

convergence
The harmonization of operational risk management activities that have similar objectives and outcomes.

corrective maintenance
A process of correcting and repairing problems that degrade the operational capability of facility services. [EC]

cost of resilience
An accumulation of expense and capital costs related to providing resilience services and achieving resilience requirements. [FRM]

coverage*
The extent to which objective evidence gathered addresses both the model and organizational scope of an appraisal. [ARC V1.1]

coverage criteria*
The specific criteria that must be satisfied in order for coverage to be claimed. [ARC V1.1]

credentialing
A process for identifying, acquiring, and maintaining access for first responders (vital staff members) from governmental authorities. [PM]

crisis
An incident in which the impact to the organization is imminent or immediate. A crisis requires immediate organizational action because the effect of the incident is already felt by the organization and must be limited or contained. [IMC]

critical success factors
The key areas in which favorable results are necessary to achieve goals. They are both internal and external to the organization. They can originate in the organization's particular industry and with its peers, in its operating environment, from temporary barriers, challenges, or problems, or from the various domains of organizational management. [RRD]

cross-training
Training in different roles or responsibilities within the organization, thus preparing staff to accept and perform new roles, however temporary, until a return to business as usual can be accomplished. [PM]

cryptographic controls
Encryption of data and information that provides an additional layer of control over information assets by ensuring that access is limited to those who have the appropriate deciphering keys. [KIM]

custodian
See "asset custodian."

defined process
A managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines; has a maintained process description; and contributes work products, measures, and other process improvement information to organizational process assets. [OPD] (See related glossary terms "managed process" and "organization's set of standard processes.")

deprovisioning
The process of revoking or removing an identity's access to organizational assets. [AM] (See related glossary term "provisioning.")

derived measures
Data obtained by combining two or more base measures. For example, the percentage of risk mitigation plans completed on time in the last 12 months is a derived measure. [MA]

direct artifact*
The tangible outputs resulting directly from implementation of a specific or generic model practice. (See related glossary terms “artifact” and “indirect artifact.”)

discovery-based appraisal*
An appraisal in which limited objective evidence is provided by the appraised organization prior to the appraisal, forcing the appraisal team to probe and uncover a majority of the objective evidence necessary to obtain sufficient coverage of the reference model practices. Discovery-based appraisals typically involve substantially greater appraisal team effort than verification-based appraisals, in which much of the objective evidence is provided by the appraised organization. (See “verification-based appraisal” for contrast.)

disposition
The appropriate and proper retirement of an asset at the end of its useful life. [KIM] [RISK]

encryption policies
Policies that govern the use of cryptographic technologies as appropriate or required for each level of information asset categorization. Includes organizational policies that manage the assignment of use, storage, disposal, and protection of cryptographic keys (such as public and private keys). [KIM]

enterprise
Synonymous with “organization.”

Enterprise Focus (EF)
An enterprise process area in CERT-RMM. The purpose of Enterprise Focus is to establish sponsorship, strategic planning, and governance over the operational resilience management process.

enterprise-level resilience requirement
Resilience requirements that reflect enterprise-level needs, expectations, and constraints. These requirements affect nearly all aspects of an organization’s operations. [RRD]

Environmental Control (EC)
An operations process area in CERT-RMM. The purpose of Environmental Control is to establish and manage an appropriate level of physical, environmental, and geographical controls to support the resilient operations of services in organizational facilities.

establish and maintain
Whenever “establish and maintain” is used in a specific practice, it refers not only to the development and maintenance of the object of the practice (such as a policy) but also to the documentation of the object and observable usage of the object. For example, “Establish and maintain an organizational policy for planning and performing the organizational process focus process area” means that not only must a policy be formulated, but it also must be documented, and it must be used throughout the organization.

event
One or more occurrences that affect organizational assets and have the potential to disrupt operations. [IMC] (See related glossary term “incident.”)

event triage
The process of categorizing, correlating, and prioritizing events with the objective of assigning events to incident handling and response. [IMC]

exercise
The testing of a service continuity plan on a regular basis to ensure that it will achieve its stated objectives when executed as the result of a disruption or interruption. [SC]

expected component
A model component that explains what may be done to satisfy a required CERT-RMM component. Specific and generic practices are expected model components. Model users can implement the expected components explicitly or implement equivalent alternative practices. (See related glossary terms “informative component” and “required component.”)

External Dependencies Management (EXD)
An operations process area in CERT-RMM. The purpose of External Dependencies Management is to establish and manage an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities.

external dependency
An external dependency exists when an external entity has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to one or more assets or services of the organization. [EXD] (See related glossary term “external entity.”)

external entity
An individual, business, or business unit (such as a customer, a contractor, or another group within the same enterprise) that is external to and in a supporting or influencing relationship with the organization that is using a process area. [EXD]

facility
Any tangible and physical asset that is part of the organization’s physical plant. Facilities include office buildings, warehouses, data centers, and other physical structures. [ADM] [EC]

federation
The assembled identity of an object across organizational units, organizations, systems, or other domains where the object has multiple identities. [ID]

Financial Resource Management (FRM)
An enterprise process area in CERT-RMM. The purpose of Financial Resource Management is to request, receive, manage, and apply financial resources to support resilience objectives and requirements.

findings*
The conclusion of an appraisal, evaluation, audit, review, or appraisal that identify the most important issues, problems, or opportunities within the appraisal scope. (See related glossary term “appraisal findings.”)

first responder
Vital staff trained to conduct damage assessment after a disruption and recommend a path to re-establishing the high-value services of the organization. [PM]

Fully Implemented (FI)*
A characterization assigned to a practice instantiation. (See CERT-RMM CAM Section 2.4.2.)

functional monitoring requirements
Requirements that describe, at a detailed level, what must be performed to meet the monitoring requirement. Specific infrastructure needs are a type of functional monitoring requirement. [MON]

fuzz testing
A means of testing that causes a software program to consume deliberately malformed data to see how the program reacts [Microsoft 2009]. [RTSE]

generic goal
A required model component that describes characteristics that must be present to institutionalize processes that implement a process area. (See related glossary term “institutionalization.”)

generic practice
An expected model component that is considered important in achieving the associated generic goal. The generic practices associated with a generic goal describe the activities that are expected to result in achievement of the generic goal and contribute to the institutionalization of the processes associated with a process area.

generic practice elaboration
An informative model component that appears after a generic practice to provide guidance on how the generic practice should be applied to the process area.

geographical dispersion
The specific and planned dispersion or scattering of physical structures and facilities so that they are not all affected by a single event or incident. [EC]

governance
An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. [EF]

high-value assets
People, information, technology, or facilities on whose availability, confidentiality, integrity, and productivity a high-value service is dependent. [ADM]

high-value services
Services on which the success of the organization’s mission depends. [RRD] [EF]

Human Resource Management (HRM)
An enterprise process area in CERT-RMM. The purpose of Human Resource Management is to manage the employment life cycle and performance of staff in a manner that contributes to the organization's ability to manage operational resilience.

identity
Documentation of certain information about a person, object, or entity that may require access to organizational assets to fulfill its role in executing services. [ID]

identity community
Defines the baseline population of persons, objects, and entities—internal and external to the organization—that could be or are authorized to access and use organizational assets commensurate with their job responsibilities and roles. Also, the collection of the organization's identity profiles. [ID]

Identity Management (ID)
An operations process area in CERT-RMM. The purpose of Identity Management is to create, maintain, and deactivate identities and associated attributes that provide access to organizational assets.

identity management
A process that addresses the management of the life cycle of objects (typically people, but often systems, devices, or other processes) that need some level of trusted access to organizational assets. [ID]

identity profile
Documentation of all of the relevant information necessary to describe the unique attributes, roles, and responsibilities of the associated person, object, or entity. [ID]

identity registration
The process of making an identity "known" to the organization as a person, object, or entity that may require access to organizational assets and that may need to be authenticated and authorized to use access privileges. [ID]

identity repository
A common accessible information repository that provides a single (or virtual) consistent source of information about organizational identities. [ID]

impact valuation
Determines the extent of the impact of operational risk using the organization's risk measurement criteria. [RISK]

incident
An event (or series of events) of higher magnitude that significantly affects organizational assets and requires the organization to respond in some way to prevent or limit organizational impact. [IMC]

incident closure
The retirement of an incident that has been responded to (i.e., there are no further actions required, and the organization is satisfied with the result) and for which the organization has performed a formal post-incident review. [IMC]

incident escalation
The process of notifying relevant stakeholders about an incident that requires an organizational response and involves stakeholder actions to implement, manage, and bring to closure with an appropriate and timely solution. [IMC]

incident life cycle
The life cycle of an incident from detection to closure. Collectively, the processes of logging, tracking, documenting, escalating and notifying, gathering and preserving evidence, and closing incidents. [IMC]

Incident Management and Control (IMC)
An operations process area in CERT-RMM. The purpose of Incident Management and Control is to establish processes to identify and analyze events, detect incidents, and determine an appropriate organizational response.

incident owner
The individuals or teams to whom an incident is assigned for containment, analysis, and response. [IMC]

incident response
The actions the organization takes to prevent or contain the impact of an incident to the organization while it is occurring or shortly after it has occurred. [IMC]

incident stakeholder
A person or organization that has a vested interest in the management of an incident throughout its life cycle. [IMC]

indirect artifact*
An artifact that is a consequence of performing a specific or generic model practice or that substantiates its implementation, but which is not the purpose for which the practice is performed. (See related glossary terms “artifact” and “direct artifact.”)

information asset
Information or data that is of value to the organization, including diverse information such as patient records, intellectual property, customer information, and contracts. [ADM] [KIM]

information asset baseline
A foundational configuration of an information asset from which changes to the asset can be detected over its life cycle. [KIM]

information asset categorization
A process for labeling and handling the sensitivity of information assets, typically based on a categorization taxonomy or scheme. [KIM]

information asset container
A technical or physical asset or a person in or on which information is stored, transported, or processed. [ADM] [KIM]

information asset owner
See related glossary term "asset owner." [ADM]

informative component
A model component that helps model users understand required and expected components. (See related glossary terms "expected component" and "required component.") Informative components can contain examples, detailed explanations, or other helpful information. Subpractices, notes, references, goal titles, practice titles, sources, typical work products, amplifications, and generic practice elaborations are informative model components.

inheritance*
Practices that are performed on behalf of a subunit entity by a superunit entity within the organization, for example, policies and procedures developed, disseminated, and administered by a superunit of the organization to serve wholly or partially the subunit entity.

instantiation*
The implementation of a model practice used in the appropriate context within the boundaries of an organizational unit. [MDD V1.2]

institutionalization
Incorporation into the ingrained way of doing business that an organization follows routinely as part of its corporate culture.

integrity
For an asset, the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner. [KIM] [TM]

intellectual property
The unique information assets of the organization that are created by the organization and are vital to its success. Intellectual property may include trade secrets, formulas, trademarks, and other organizationally produced assets. [KIM]

internal control system
The methods, policies, and procedures used to protect and sustain high-value assets at a level commensurate with their role in supporting organizational services. [KIM] (See related glossary term "high-value assets.")

key control indicators
Organizationally specific indicators that provide information about the effectiveness of the organization's internal control system. [EF]

key performance indicators
Organizationally specific performance metrics that measure progress against the organization's strategic objectives and critical success factors. [EF]

key risk indicators
Organizationally specific thresholds that, when crossed, indicate levels of risk that may be outside of the organization's risk tolerance. [EF] [RISK]

Knowledge and Information Management (KIM)
An operations process area in CERT-RMM. The purpose of Knowledge and Information Management is to establish and manage an appropriate level of controls to support the confidentiality, integrity, and availability of the organization's information, vital records, and intellectual property.

Largely Implemented (LI)*
A characterization assigned to a practice instantiation. (See CERT-RMM CAM Section 2.4.2.)

lead appraiser*
A person who has achieved recognition from an authorizing body to perform as an appraisal team leader for a particular appraisal method. [ARC V1.1]

line of business
A logical grouping of organizational units that have a common purpose, such as production of products for a particular market segment.

managed process
A performed process that is planned and executed in accordance with policy; employs skilled people having adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled, and reviewed; and is evaluated for adherence to its process description. (See related glossary term "performed process.")

Measurement and Analysis (MA)
A process management process area in CERT-RMM. The purpose of Measurement and Analysis is to develop and sustain a measurement capability that is used to support management information needs for managing the operational resilience management process.

measurement objectives
Documents the purpose for which measurements and analysis are done and specifies the kinds of actions that may be taken based on the results of data analysis. [MA]

measures
Measurements of the resilience process that may be categorized by obtaining direct measurements (base measures) or by obtaining measurements that are a combination of two or more base measures (derived measures). [MA]

misuse/abuse case
A descriptive statement of the undesirable, nonstandard conditions that software is likely to face during its operation from either unintentional misuse or intentional and malicious misuse or abuse. [RTSE]

model scope*
The parts of CERT-RMM that will be used to guide the improvement effort. In an appraisal the model scope is the part of CERT-RMM that will be used as the basis within which the processes to be investigated operate.

Monitoring (MON)
A process management process area in CERT-RMM. The purpose of Monitoring is to collect, record, and distribute information about the operational resilience management process to the organization on a timely basis.

monitoring infrastructure
The technologies and support services that are needed to support the achievement of monitoring requirements. [MON]

monitoring requirements
The requirements established to determine the information gathering and dissemination needs of stakeholders. [MON]

monitoring stakeholder
A person or group that has a vested interest in being involved in or a beneficiary of the organization's monitoring activities. [MON]

Not Implemented (NI)*
A characterization assigned to a practice instantiation. (See CERT-RMM CAM Section 2.4.2.)

Not Yet (NY)*
A characterization assigned to a practice instantiation. (See CERT-RMM CAM Section 2.4.2.)

objective evidence*
Documents or interview results used as indictors of the implementation or institutionalization of model practices. (See related glossary term "practice implementation indicator.")

operational constraint
A limit imposed on an organization's operational activities. These limits can be imposed by the organization on itself or can come from the organization's operating environment (e.g., regulations). [RRD]

operational resilience
The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk. (See related glossary term "operational risk.")

operational resilience management
The processes by which an organization designs, develops, implements, manages, and improves strategies for protecting and sustaining high-value services and associated assets such as people, information, technology, and facilities.

operational resilience requirements
Refers collectively to requirements that ensure the protection of high-value assets as well as their continuity when a disruptive event has occurred. The requirements traditionally encompass security, business continuity, and IT operational requirements. These include the security objectives for information assets (confidentiality, integrity, and availability) as well as the requirements for business continuity planning and recovery and the availability and support requirements of the organization's technical infrastructure. [RRD]

operational risk
The potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events.

operational risk taxonomy
The collection and cataloging of common operational risks that the organization is subjected to and must manage. The risk taxonomy is a means for communicating these risks and for developing organizational unit and line of business-specific mitigation actions if operational assets and services are affected by them. [RISK]

organization
An administrative structure in which people collectively manage one or more services as a whole, and whose services share a senior manager and operate under the same policies. May consist of many organizations in many locations with different customers. (See related glossary terms "enterprise" and "organizational unit.")

organizational asset
See "asset."

organizational impact area
See "area of impact."

organizational process assets
Artifacts that relate to describing, implementing, and improving processes (e.g., policies, measurements, process descriptions, and process implementation support tools). The term "process assets" is used to indicate that these artifacts are developed or acquired to meet the business objectives of the organization, and they represent investments by the organization that are expected to provide current and future business value. (See related glossary term "process asset library.")

Organizational Process Definition (OPD)
A process management process area in CERT-RMM. The purpose of Organizational Process Definition is to establish and maintain a usable set of organizational process assets and work environment standards for operational resilience.

Organizational Process Focus (OPF)
A process management process area in CERT-RMM. The purpose of Organizational Process Focus is to plan, implement, and deploy organizational process improvements based on a thorough understanding of current strengths and weaknesses of the organization's operational resilience processes and process assets.

organizational process maturity
In models with a staged representation, organizational process maturity is measured by the degree of process improvement across predefined sets of process areas. Since CERT-RMM does not have a staged representation, characterization of organizational process maturity can only be implied by reaching successively higher levels of capability across CERT-RMM process areas.

organizational scope*
The part of the organization that is the focus of the CERT-RMM deployment. In an appraisal the organizational scope is the collection of organizational units that provides instantiations used within, and representative of, an organizational unit.

organizational sensitivity
The degree to which access to an information asset must be limited due to confidentiality or privacy requirements. [ADM]

Organizational Training and Awareness (OTA)
An enterprise process area in CERT-RMM. The purpose of Organizational Training and Awareness is to promote awareness and develop skills and knowledge of people in support of their roles in attaining and sustaining operational resilience.

organizational subunit
Any subelement of the organizational unit. An organizational subunit is fully contained within the organizational unit.

organizational superunit
Any part of the organization that is at a higher level than the organizational unit. Organizational superunit can also be used to refer to the entire organization.

organizational unit (OU)
A distinct subset of an organization or enterprise. An organizational unit is typically part of a larger organization, although in a small organization the organizational unit may be the whole organization.

organizationally high-value services
Services on which the success of the organization's mission is dependent. [RRD] [EF]

organization's process asset library
A library of information used to store and make available process assets that are useful to those who are defining, implementing, and managing processes in the organization. This library contains process assets that include process-related documentation such as policies, defined processes, checklists, lessons-learned documents, templates, standards, procedures, plans, and training materials.

organization's set of standard processes
A collection of definitions of the processes that guide activities in an organization. These process descriptions cover the fundamental process elements (and their relationships to each other, such as ordering and interfaces) that must be incorporated into the defined processes that are implemented in projects across the organization. A standard process enables consistent development and

maintenance activities across the organization and is essential for long-term stability and improvement. [OPD] (See related glossary terms “defined process” and “process element.”)

Partially Implemented (PI)*
A characterization assigned to a practice instantiation. (See CERT-RMM CAM Section 2.4.2.)

people
All staff, both internal and external to the organization, and all managers employed in some manner by the organization to perform a role or fulfill a responsibility that contributes to meeting the organization’s goals and objectives. [PM]

People Management (PM)
An operations process area in CERT-RMM. The purpose of People Management is to establish and manage the contributions and availability of people to support the resilient operation of organizational services.

perfective maintenance
Maintenance performed by acquiring additional or improved operational capacity. [EC]

performed process
A process that accomplishes the needed work to produce work products. The specific goals of the process area are satisfied.

physical control
A type of control that prevents physical access to and modification of information assets or physical access to technology and facilities. Physical controls often include such artifacts as card readers and physical barrier methods. [KIM] [TM] [EC]

planned downtime
Acceptable and planned interruption of the availability of an information or technology asset, usually as the result of a user- or management-initiated event. [TM]

post-incident review
A formal part of the incident closure process that refers to the organization’s formal examination of the causes of an incident and the ways in which the organization responded to it, as well as the administrative, technical, and physical control weaknesses that may have allowed the incident to occur. [IMC]

Practice Implementation Indicator (PII)*
An objective attribute or characteristic used as a footprint to verify the conduct of an activity or implementation of a model specific or generic practice. (See related glossary term “objective evidence.”)

preliminary findings
Findings created by the appraisal team after synthesizing objective evidence. Preliminary findings are provided to appraisal participants for validation. (See related glossary terms “appraisal findings” and “findings.”)

preventive maintenance
Preplanned activities performed to prevent potential facility problems from occurring. [EC]

privacy
The assurance that information about an individual is disclosed only to people, processes, and devices authorized by that individual or permitted under privacy laws and regulations. [KIM]

privilege
See "access privilege." [AM]

problem management
The process that an organization uses to identify recurring problems, examine root causes, and develop solutions for these problems to prevent future, similar incidents. [IMC]

process
Activities that can be recognized as implementations of practices in the model. These activities can be mapped to one or more practices in process areas to allow the model to be useful for process improvement and process appraisal. (See related glossary terms "process area," "subprocess," and "process element.") There is a special use of the phrase "the process" in the statements and descriptions of the generic goals and generic practices. In that context, "the process" is the process or processes that implement the process area.

process architecture
The ordering, interfaces, interdependencies, and other relationships among the process elements in a standard process. Process architecture also describes the interfaces, interdependencies, and other relationships between process elements and external processes (e.g., contract management). [OPD]

process area
A cluster of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making improvement in that area.

process asset library
A collection of process asset holdings that can be used by an organization or project. (See related glossary term "organization's process asset library.")

process capability
The range of expected results that can be achieved by following a process. The generic goals and practices define the degree to which a process is institutionalized; capability levels indicate the degree to which a process is institutionalized.

process element
The fundamental unit of a process. A process can be defined in terms of subprocesses or process elements. A subprocess can be further decomposed into subprocesses or process elements; a process element cannot. (See related glossary term "subprocess.") Each process element covers a closely related set of activities (e.g., estimating element, peer review element). Process elements can be portrayed using templates to be completed, abstractions to be refined, or descriptions to be modified or used. A process element can be an activity or a task. [OPD]

process performance
A measure of actual results achieved by following a process. It is characterized by both process measures (e.g., vulnerabilities eliminated before being exploited) and product or service measures (e.g., control system network unavailability due to exploited vulnerabilities).

protection strategy
The strategy, related controls, and activities necessary to protect an asset from undesired harm or disruptive events. The protection strategy is relative to the conditions to which the asset is subjected. (See related glossary term “condition.”)

provisioning
The process of assigning or activating an identity profile and its associated roles and access privileges. [ID]

proximity
The relative distance between facilities, which is a consideration in collocation and geographical dispersion. [EC] (See related glossary terms “collocation” and “geographical dispersion.”)

public infrastructure
Infrastructure owned by the community in the geographical area that contains a facility. Includes telecommunications and telephone services, electricity, natural gas, and other energy sources, as well as water and sewer services, trash collection and disposal, and other support services. [EC]

public services
Services that are provided in the community or in the geographical area that contains a facility. Includes fire response and rescue services, local and federal law enforcement, emergency management services such as paramedics and first responders, and animal control. [EC]

rating*
See “appraisal rating.”

Recovery Point Objective (RPO)
Establishes the point to which an information or technology asset (typically an application system) must be restored to allow recovery of the asset and associated services after a disruption. [TM]

Recovery Time Objective (RTO)
Establishes the period of acceptable downtime of an information or technology asset after which the organization would suffer an unwanted consequence or impact. [TM]

regulation
A type of compliance obligation issued by a governmental, regulatory, or other agency. [COMP]

release build
A version of an information or technology asset that is to be released into production; an object in the release management process. [KIM] [TM]

release management
The process of managing successive release of versions of information and technology assets into an operations and production environment. [KIM] [TM]

required component
A CERT-RMM component that is essential to achieving process improvement in a given process area. Required components are used in appraisals to determine process capability. Specific goals and generic goals are required components. (See related glossary terms “expected component” and “informative component.”)

residual risk
The risk that remains and is accepted by the organization after mitigation plans are implemented. [RISK]

resilience
See “operational resilience.”

resilience budget
A budget specifically developed and funded to support the organization’s resilience activities. [FRM]

resilience management
See “operational resilience management.”

resilience obligations
An understanding of a commitment, promise, or duty to follow and enforce the resilience requirements of the organization. [HRM]

resilience requirement
A constraint that the organization places on the productive capability of an asset to ensure that it remains viable and sustainable when charged into production to support a service.

Resilience Requirements Development (RRD)
An engineering process area in CERT-RMM. The purpose of Resilience Requirements Development is to identify, document, and analyze the operational resilience requirements for high-value services and related assets.

Resilience Requirements Management (RRM)
An engineering process area in CERT-RMM. The purpose of Resilience Requirements Management is to manage the resilience requirements of high-value services and associated assets and to identify inconsistencies between these requirements and the activities that the organization performs to meet the requirements.

resilience specifications
Criteria that the organization establishes for a working relationship with an external entity, which may be incorporated into contractual terms. Typically include the resilience requirements of any of the organization’s high-value assets and services that are placed in the external entity’s control. Also may include required characteristics of the external entity (e.g., financial condition and experience), required behaviors of the external entity (e.g., security and training practices), and

performance parameters that must be exhibited by the external entity (e.g., recovery time after an incident and response time to service calls).

resilience staff
Internal or external staff who are specifically involved in or assigned to resilience-focused activities that are typically found in security, business continuity, and IT operations disciplines. [OTA]

resilience training
The process and activities focused on imparting the necessary skills and knowledge to people for performing their roles and responsibilities in support of the organization's operational resilience management process. [OTA]

resilience training needs
Training requirements related to the skills and competencies required at a tactical level to carry out the activities required for managing operational resilience. [OTA]

Resilient Technical Solution Engineering (RTSE)
An engineering process area in CERT-RMM. The purpose of Resilient Technical Solution Engineering is to ensure that software and systems are developed to satisfy their resilience requirements.

return on resilience investment (RORI)
The return on investment for funding resilience activities. Provides a way to justify resilience costs and provides direct support for the contribution that managing operational resilience makes in achieving strategic objectives. [FRM]

risk
The possibility of suffering harm or loss. From a resilience perspective, risk is the combination of a threat or vulnerability (condition) and the impact (consequence) to the organization if the threat or vulnerability is exploited. In CERT-RMM, this definition is typically applied to the asset or service level such that risk is the possibility of suffering harm or loss due to disruption of high-value assets and services. [RISK]

risk analysis
A risk management process focused on understanding the condition and consequences of risk, prioritizing risks, and determining a path for addressing risks. Determines the importance of each identified operational risk and is used to facilitate the organization's risk disposition and mitigation activities. [RISK]

risk appetite
An organization's stated level of risk aversion. Informs the development of risk evaluation criteria in areas of impact for the organization. [RISK] (See related glossary terms "area of impact," "risk measurement criteria," and "risk tolerance.")

risk category
An organizationally defined description of risk that typically aligns with the various sources of operational risk but can be tailored to the organization's unique risk environment. Risk categories

provide a means to collect and organize risks to assist in the analysis and mitigation processes. [RISK]

risk disposition
A statement of the organization's intention for addressing an operational risk. Typically limited to accept, transfer, research, or mitigate. [RISK]

Risk Management (RISK)
An enterprise process area in CERT-RMM. The purpose of Risk Management is to identify, analyze, and mitigate risks to organizational assets that could adversely affect the operation and delivery of services.

risk management
The continuous process of identifying, analyzing, and mitigating risks to organizational assets that could adversely affect the operation and delivery of services. [RISK]

risk measurement criteria
Objective criteria that the organization use for evaluating, categorizing, and prioritizing operational risks based on areas of impact. [RISK] (See related glossary term "area of impact.")

risk mitigation
The act of reducing risk to an acceptable level. [RISK]

risk mitigation plan
A strategy for mitigating risk that seeks to minimize the risk to an acceptable level. [RISK]

risk parameter (risk management parameter)
Organizationally specific risk tolerances used for consistent measurement of risk across the organization. Risk parameters include risk tolerances and risk measurement criteria. [RISK] (See related glossary terms "risk tolerance" and "risk measurement criteria.")

risk statement
A statement that clearly articulates the context, conditions, and consequences of risk. [RISK]

risk taxonomy
See "operational risk taxonomy."

risk threshold
An organizationally developed type of risk parameter that is used by management to determine when a risk is in control or when it has exceeded acceptable organizational limits. [RISK]

risk tolerance
Thresholds that reflect the organization's level of risk aversion by providing levels of acceptable risk in each operational risk category that the organization established. Risk tolerance, as a risk parameter, also establishes the organization's philosophy on risk management—how risks will be controlled, who has the authorization to accept risk on behalf of the organization, and how often and to what degree operational risk should be assessed. [RISK]

RMM steward*
See “CERT-RMM steward.”

root cause analysis
An approach for determining the underlying causes of events or problems as a means of addressing the symptoms of such events as they manifest in organizational disruptions. [VAR]

scope
See “appraisal scope,” “model scope,” and “organizational scope.”

secure design pattern
A general, reusable solution to a commonly occurring problem in design. A design pattern is not a finished design that can be transformed directly into code. It is a description or template for how to solve a problem that can be used in many different situations. Secure design patterns are meant to eliminate the accidental insertion of vulnerabilities into code or to mitigate the consequences of vulnerabilities. Secure design patterns address security issues at widely varying levels of specificity, ranging from architectural-level patterns involving the high-level design of the system down to implementation-level patterns providing guidance on how to implement portions of functions or methods in the system [Dougherty 2009]. [RTSE]

sensitivity
A measure of the degree to which an information asset must be protected based on the consequences of its unauthorized access, modification, or disclosure. [KIM]

service
A set of activities that the organization carries out in the performance of a duty or in the production of a product. [ADM] [EF] (See related glossary term “business process.”)

Service Continuity (SC)
An engineering process area in CERT-RMM. The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

service continuity plan (business continuity plan)
A service-specific plan for sustaining services and associated assets under degraded conditions. [SC]

service level agreement (SLA)
A type of agreement that specifies levels of service expected from business partners in the performance of a contract or agreement. In CERT-RMM, SLAs are expanded to include the satisfaction of resilience requirements by business partners when one or more organizational assets are in their custodial care.

service-level resilience requirements
Service requirements established by owners of the service such as an organizational unit or a line of business. [RRD] (See related glossary term “asset-level resilience requirements.”)

service profile
A profile that describes services in sufficient detail to capture the activities, tasks, and expected outcomes of the services and the assets that are vital to the service. [EF]

service resilience requirements
Resilience needs of a service in its pursuit of its mission. Resilience requirements for services primarily address availability and recoverability but are also directly related to the confidentiality, integrity, and availability requirements of associated assets. [RRD]

services map
Details the relationships between a service, associated business processes, and associated assets. [RRD]

shared resilience requirements
Shared requirements are those that are developed for shared organizational assets such as a facility in which more than one high-value service is executed. [RRD]

skills inventory or repository
A means for identifying and documenting the current skill set of the organization's human resources. [HRM]

specific goal
A required model component that describes the unique characteristics that must be present to satisfy the process area. (See related glossary terms "process area" and "required component.")

specific practice
An expected model component that is considered important in achieving the associated specific goal. The specific practices describe the activities expected to result in achievement of the specific goals of a process area. (See related glossary terms "expected component," "process area," and "specific goal.")

staff
All people, both internal and external to the organization, employed in some manner by the organization to perform a role or fulfill a responsibility that contributes to meeting the organization's goals and objectives. Does not include those in managerial roles.

stakeholder
A person or organization that has a vested interest in the organization or its activities. (See related glossary terms "communications stakeholder" and "monitoring stakeholder.")

standard process
An operational definition of the basic process that guides the establishment of a common process in an organization. A standard process describes the fundamental process elements that are expected to be incorporated into any defined process. It also describes relationships (e.g., ordering, interfaces) among these process elements. [OPD] (See related glossary term "defined process.")

strategic objectives (strategic drivers)
Strategic objectives are the performance targets that the organization sets to accomplish its mission, vision, values, and purpose. [EF]

strategic planning
The process of developing strategic objectives and plans for meeting these objectives. [EF]

strength*
Exemplary or noteworthy implementation of a model practice. (See related glossary term "weakness" for contrast.) [ARC Vv1.1]

subprocess
A process that is part of a larger process. A subprocess can be decomposed into subprocesses or process elements. [OPD] (See related glossary terms "process" and "process element.")

succession planning
A form of continuity planning for vital staff and/or decision-making management focused on providing a smooth transition for vital roles and sustaining the high-value services of the organization. [PM]

sufficient coverage*
In the case of an appraisal, "sufficient" is used to determine if coverage requirements have been met. See "coverage criteria" and "adequate."

supplier
An internal or external organization or contractor who supplies key products and services to the organization to contribute to accomplishing the missions of its high-value services.

sustain
Maintain in a desired operational state.

sustainment strategy
The strategy, related controls, and activities necessary to sustain an asset when it is subjected to undesired harm or disruptive events. The sustainment strategy is relative to the consequences to the organization if the asset is harmed or disrupted.

tailoring*
See "appraisal tailoring."

technical control
A type of technical mechanism that supports protection methods for assets such as firewalls and electronic access controls. [KIM] [TM]

technology asset
Any hardware, software, or firmware used by the organization in the delivery of services. [TM]

technology interoperability
The ability of technology assets to exist and operate in a connected manner to meet an organizational goal, objective, or mission. [TM]

Technology Management (TM)
An operations process area in CERT-RMM. The purpose of Technology Management is to establish and manage an appropriate level of controls related to the integrity and availability of technology assets to support the resilient operations of organizational services.

threat
A situation, vulnerability, or condition that can be exploited to produce an unexpected or unwanted outcome for the organization. [RISK] [VAR]

threat actor
A person or event that has the potential to exploit a threat. [VAR] [RISK]

threat environment
The set of all types of threats that could affect the current operations of the organization. (See related glossary term “threat.”)

threat motive
The reason that a threat actor would exploit a vulnerability or threat. [VAR] [RISK]

unplanned downtime
Interruption in the availability of an information or technology asset (and in some cases, a facility asset) due to an unplanned event or incident, often resulting from diminished operational resilience. [TM]

user
Any entity or object that the organization has granted some form of access to an organizational asset. Typically referred to as an “identity.” (See related glossary term “identity.”)

verification-based appraisal*
An appraisal in which the focus of the appraisal team is on verifying the set of objective evidence provided by the appraised organization in advance of the appraisal in order to reduce the amount of probing and discovery of objective evidence during the appraisal on-site period. (See “discovery-based appraisal” for contrast.)

vital records
A record that must be preserved and available for retrieval if needed. This refers to records or documents that, for legal, regulatory, or operational reasons, cannot be irretrievably lost or damaged without materially impairing the organization’s ability to conduct business. [KIM]

vital staff
A select group of individuals who are absolutely essential to the sustained operation of the organization, particularly under stressful conditions. [PM]

vulnerability
A potential exposure or weakness that could be exploited. The susceptibility of an organizational service or asset to disruption. [VAR]

Vulnerability Analysis and Resolution (VAR)
An operations process area in CERT-RMM. The purpose of Vulnerability Analysis and Resolution is to identify, analyze, and manage vulnerabilities in an organization's operating environment.

vulnerability management strategy
A strategy for identifying and reducing exposure to known vulnerabilities. [VAR]

vulnerability repository
An organizational inventory of known vulnerabilities. [VAR]

vulnerability resolution
The action that the organization takes to reduce or eliminate exposure to vulnerability. [VAR]

waiver
Documentation for staff members who have been exempted from awareness training or other activities for any reason. Such documentation includes the rationale for the waiver and approval by the individual's manager (or similarly appropriate person). Each required course should include criteria for granting training waivers. [OTA]

weakness*
The ineffective, or lack of, implementation of one or more model practices. (See related glossary term "strength" for contrast.) [ARC V1.1]

References/Bibliography

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

[Caralli 2010]
Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; & Young, Lisa R. *CERT® Resilience Management Model, v1.0* (CMU/SEI-2010-TR-012). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm

[Chrissis 2007]
Chrissis, Mary Beth; Konrad, Mike; & Shrum, Sandy. *CMMI® Second Edition: Guidelines for Process Integration and Product Improvement*. Addison-Wesley, 2007.

[CMMI 2001]
CMMI Product Team. *Appraisal Requirements for CMMI, Version 1.1* (CMU/SEI-2001-TR-034, ADA 339208). Software Engineering Institute, Carnegie Mellon University, 2001. http://www.sei.cmu.edu/reports/01tr034.pdf

[Humphrey 1989]
Humphrey, Watts. *Managing the Software Process*. Addison-Wesley, 1989.

[Radice 2005]
Radice, Ron. *Interpreting SCAMPI for a People CMM Appraisal at Tata Consultancy Services* (CMU/SEI-2005-SR-001). Software Engineering Institute, Carnegie Mellon University, 2005.

[SCAMPI 2006]
SCAMPI A Upgrade Team, *Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠) A, Version 1.2: Method Definition Document* (CMU/SEI-2006-HB-002). Software Engineering Institute, Carnegie Mellon University, 2006.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	October 2011	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
CERT® Resilience Management Model Capability Appraisal Method (CAM) Version 1.1	FA8721-05-C-0003

6. AUTHOR(S)
Resilient Enterprise Management Team

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2011-TR-020

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-2011-020

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

The CERT® Resilience Management Model (CERT®-RMM), developed by the CERT® Program at Carnegie Mellon University's Software Engineering Institute (SEI), 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. In operational terms, resilience is an *emergent* property of an organization that can continue to carry out its mission after a disruption that does not exceed its operational limit.

The ability of an organization to assess its current level of capability using CERT-RMM as the reference model is essential for measuring the current competency of its operational practices, setting improvement targets, and establishing plans and actions to close any gaps.

The SEI has developed and maintained the Standard Capability Maturity Model® Integration (CMMI®) Appraisal Method for Process Improvement (SCAMPISM) family of appraisal methods from the CMMI product suite. Consultations with the SEI's CMMI program manager indicated that it would be appropriate to extend the pedigree of the SCAMPI family of appraisal methodologies for the CERT-RMM Capability Appraisal Method (CAM) Version 1.1.

This report demonstrates that the SCAMPI Version 1.2 method can be adapted and applied to CERT-RMM V1.1 as the reference model for a process appraisal.

14. SUBJECT TERMS	15. NUMBER OF PAGES
CERT Resilience Management Model, CERT RMM version 1.1, appraisal, capability appraisal method, process improvement, maturity model, CAM	112

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL