Software Engineering Institute

Measuring Operational Resilience Using the CERT® Resilience Management Model

Julia H. Allen
Noopur Davis

September 2010

TECHNICAL NOTE
CMU/SEI-2010-TN-030

CERT Program

http://www.sei.cmu.edu

Carnegie Mellon

This report was prepared for the

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

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

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

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

Table of Contents

List of Figures

List of Tables

Acknowledgments

The authors would like to thank the following reviewers of this report who generously contributed their time, knowledge, and experience to provide comments that greatly enhanced the clarity and accuracy of the concepts presented:

- Christopher Alberts, SEI
- Richard Barbour, SEI
- Pamela Curtis, SEI
- Summer Fowler, SEI
- Nader Mehravari, Lockheed Martin
- James Stevens, SEI
- Robert Stoddard, SEI
- Elizabeth Sumpter, NSA
- Lisa Young, SEI

The authors would also like to thank Richard Caralli, the technical manager of the Resilience Enterprise Management team and the architect of the CERT-RMM, for his encouragement, thought leadership, and sponsorship of this work.

Abstract

Measurement involves transforming management decisions, such as strategic direction and policy, into action, and measuring the performance of that action. As organizations strive to improve their ability to effectively manage operational resilience, it is essential that they have an approach for determining what measures best inform the extent to which they are meeting their performance objectives. Operational resilience comprises the disciplines of security, business continuity, and aspects of IT operations.

The reference model used as the foundation for this research project is the CERT® Resilience Management Model v1.0. This model provides a process-based framework of goals and practices at four increasing levels of capability and defines twenty six process areas, each of which includes a set of candidate measures. Meaningful measurement occurs in a context so this approach is further defined by exploring and deriving example measures within the context of selected ecosystems, which are collections of process areas that are required to meet a specific objective. Example measures are defined using a measurement template.

This report is the first in a series and is intended to start a dialogue on this important topic.

1 Introduction

The purpose of this technical note is to begin a dialogue and establish a foundation for measuring and analyzing operational resilience. We define operational resilience as

> *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 [Caralli 2010a].*

and the management of operational resilience as

> *the direction and coordination of activities to achieve resilience objectives that align with the organization's strategic objectives and critical success factors [Caralli 2010d.]*

Operational resilience comprises the disciplines of security, business continuity, and some aspects of IT operations. We focus on measuring and analyzing an organization's ability to effectively manage these disciplines. Operational resilience supports the ability of services and associated assets to achieve their mission. An operationally-resilient service is a service that can meet its mission under times of disruption or stress, *and* can return to normalcy when the disruption or stress is eliminated. A service is *not* resilient if it cannot return to normal after being disrupted, even if it can temporarily withstand adverse circumstances.

Why is measurement and analysis of operational resilience important? It was the scientist Lord Kelvin who said, "When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the stage of science."[1] He also is quoted as having said "When you cannot measure it, you cannot improve it."[2]

Measurement is about transforming strategic direction, policy, and other forms of management decision into action, and measuring the performance of such action. "Visible measures provide a positive influence on human behavior by invoking the desire to succeed and compare favorably with one's peers [CISWG 2005]." The right measures express the extent to which objectives are being met (or not), how well requirements are being satisfied (or not), how well processes and controls are functioning (or not), and the extent to which performance outcomes are being achieved (or not).

The Software Engineering Institute (SEI) has engaged in software engineering measurement and analysis (SEMA) for many years. *Goal-Driven Software Measurement—A Guidebook* and the SEI's SEMA web site state the following as the foundation for measurement and analysis:

[1] http://en.wikiquote.org/wiki/William_Thomson

[2] http://zapatopi.net/kelvin/quotes/

Why measure? *Because without data, you only have opinions.*

Why analyze? *Because the data you collect can't help you if you don't understand it and use it to shape your decisions [Park 1996] [SEMA 2010].*

SEMA identifies four needs for measurement and analysis: to gain understanding of the entity being measured, to determine current status including the extent to which the entity is achieving its goals and objectives, to predict future state, and to help improve.

These four needs for measurement and analysis also apply to operational resilience. Organizations lack a reliable means for measuring either their operational resilience or their capability for managing operational resilience. Measuring the degree, state, or "posture" of an intangible quality attribute or emergent property is difficult even under normal operating conditions. Unfortunately, measuring operational resilience is most accurately done during times of stress and disruption. This is often too late to be of benefit, and the organization is typically in too reactive a mode even to consider how to improve in anticipation of the next incident. It is necessary to be able to predict how the organization will perform in the future when the threat and risk environment changes. It is necessary but not sufficient to know how well the organization responded to a single attack that occurred in the past. Looking to the fidelity and performance of the contributing processes may be a way to gain more confidence and precision about an organization's state of operational resilience—it is, at least, one important indicator that is not typically being measured today [Caralli 2010c]. This leads to the need for in-process measures, which can be collected and analyzed as processes are being performed.

As organizations strive to improve their ability to effectively manage operational resilience, determining what measures best inform their improvement programs and processes is essential. In January 2010, CERT initiated the resilience measurement and analysis research project. This report is the first in a series and is intended to start the dialogue on this important topic.

Research Questions

The resilience measurement and analysis research project is focused on addressing the following questions, often asked by business leaders:

1. How resilient is my organization?
2. Have our processes made us more resilient?

And to inform these, answering this question:

3. What should be measured to determine if process performance objectives for operational resilience are being achieved?

Consistent, timely, and accurate measurements are important feedback for managing any activity including operational resilience. However, a quote often attributed to Deming says, "If you can't describe what you are doing as a process, you don't know what you're doing."[3] And if you don't know what you are doing, measurement and analysis will not help. Attempting to measure operational resilience without a process-based definition to use as the foundation is thus not very mea-

[3] "W. Edwards Deming." BrainyQuote.com. Xplore Inc, 2010. 2 August. 2010. http://www.brainyquote.com/quotes/quotes/w/wedwardsd133510.html

ningful. The reference process model we chose for our initial work is the CERT® Resilience Management Model (CERT-RMM), which was developed by the CERT Program at Carnegie Mellon University's Software Engineering Institute [Caralli 2010a, 2010b]. This model provides a process-based framework of goals and practices at four increasing levels of capability (Incomplete, Performed, Managed, and Defined) and a companion appraisal method. It comprises 26 process areas (PAs) that define a set of practices which, when implemented collectively, satisfy a set of goals considered important for effectively managing the organization's ability to be operationally resilient. When implementing measurement and analysis (refer to the CERT-RMM Measurement and Analysis (MA)) PA the organization establishes the objectives for measurement (i.e., what it intends to accomplish) and determines the measures that are useful for managing and improving operational resilience [Caralli 2010b].

The first step in defining a meaningful measurement program for operational resilience and its effective management is to determine and express the required or desired level of operational resilience for an organization. An organization[4] may be the enterprise, a business line or operating unit of the enterprise, or any other form of business relationship that includes external entities such as partners, suppliers, and vendors. An organization can target a level of capability for one or more PAs, thus establishing a benchmark against which its operational resilience can be measured. Ideally, the targeted level for each process area is established during strategic and operational planning and when planning for continuity of operations, not as an afterthought during times of stress and service disruption. The targeted level should be no less and no more than that which is required to meet business mission objectives.

An effective measurement and analysis process includes the following activities and objectives [CMMI Product Team 2006]:

- specifying the objectives of measurement and analysis such that they are aligned with identified information needs and objectives such as those for operational resilience (refer to Section 2.2)
- specifying the measures, analysis techniques, and mechanisms for data collection, data storage, reporting, and feedback
- implementing the collection, storage, analysis, and reporting of the data
- providing objective results that can be used in making informed decisions, and taking appropriate corrective actions

Integrating measurement and analysis into the operational resilience management program supports

- planning, estimating, and executing operational resilience management activities
- tracking the performance of operational resilience management activities against established plans and objectives, including resilience requirements
- identifying and resolving issues in operational resilience management processes

[4] CERT-RMM defines organization as "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. An organization may consist of many organizations in many locations with different customers." [Caralli 2010a]

- providing a basis for incorporating measurement into additional operational resilience management processes in the future

Scope, Terminology, and Approach

The long term scope of this research project is resilience measurement and analysis, not solely CERT-RMM measurement and analysis. As stated above, we start this work with the CERT-RMM version 1.0, its 26 process areas, and companion measures at capability level 2 for each process area as the documented body of knowledge in this space and as our reference model [Caralli 2010b].

As this work develops, we plan to add better definition of terms, specificity, and precision to the dialogue. For our efforts, metric is equivalent to "number." Measure is equivalent to "number with analysis and meaning, in context." We recognize that our community often uses metric to mean both.

This report, as a first step in this research project, provides a proposed approach for identifying and selecting measures that allow decision makers to determine the extent to which they are meeting their performance objectives for operational resilience. We initially start with objectives at CERT-RMM Capability Level 2 – Managed and evaluate the example measures described in Generic Goal 2: Generic Practice 8 (GG2.GP8)[5] in each CERT-RMM v1.0 process area as the basis [Caralli 2010b]. Meaningful measurement occurs in a context so we further define this approach by exploring measures within the context of selected ecosystems, which are collections of process areas required to meet a specific objective.

Intended audience

The intended audience for this report includes those interested in measuring the extent to which their organizations are operationally resilient using CERT-RMM as the basis for the definition of operational resilience and its effective management. The report assumes that readers are familiar with CERT-RMM [Caralli 2010a, 2010b], the disciplines it covers (management of security, management of business continuity, and aspects of IT operations management), and its fundamental concepts and terminology[6]. Readers need not have a deep understanding of each of the 26 process areas, but they should be knowledgeable about the processes that compose each of the resilience disciplines and their relationships. Readers will also find it useful to have general familiarity with the use of process models as the basis for improvement.

In addition, those with a measurement and analysis background who wish to apply that background to measuring operational resilience will find this report of interest. Readers of this report will find it helpful to be familiar with the general concepts of goal-driven measurement as defined in *Goal-Driven Software Measurement—A Guidebook* [Park 1996], the SEI's Software Engineer-

[5] GG2.GP8 Monitor and Control the Process appears in all 26 CERT-RMM process areas. It presents examples of measures that can be used to assess the extent to which the process has been implemented and is effective in achieving its objectives. These measures will be updated and improved throughout the conduct of this research project.

[6] An overview of CERT-RMM is available in two archived SEI webinars: "Transforming Your Operational Resilience Management Capabilities: CERT's Resilience Management Model" and "Improving and Sustaining Processes for Managing Operational Resiliency CERT Resiliency Management Model." These are available at http://www.sei.cmu.edu/library/webinars.cfm.

ing Measurement and Analysis work [SEMA 2010], and foundational work done by Basili and Rombach (refer to Sections 2 and 3 for further details).

The intended audience for the results of this research project is decision makers responsible for managing aspects of operational resilience in their organizations. These include but are not limited to high-level managers (senior level executives and officers, senior managers), line of business and organizational unit managers, business service owners, and asset owners and custodians (assets include information, technology, facilities, and people)

Report Overview

Meaningful measurement derives from well-stated objectives, at the enterprise, organizational unit, and process level. CERT-RMM documents many of these at the process level and describes many of the enterprise and organizational aspects that need to be considered. Section 2 of this report synthesizes this content and derives six high-level objectives for managing operational resilience. Each measure that is defined in the course of this research project will map either directly to one of these objectives or indirectly to one or more measures that then map directly to an objective.

Section 3 presents the research foundations, a more detailed description of our research approach, and several measurement concepts that serve as the basis for this report and research project. These include measurement relationships and definitions (attribute to base measure to derived measure to indicator to information need), scales for resilience measures (nominal, ordinal, interval, ratio), and resilience measurement types (implementation, effectiveness, process performance). This section derives and presents a candidate template to be used in defining resilience measures along with a completed example. It also maps fields in the measurement template to two CERT-RMM process areas that describe essential goals and practices that provide a measurement capability: Measurement and Analysis (MA) and Monitoring (MON).

The objectives defined in Section 2 and the concepts and templates presented in Section 3 are applied in Section 4. This section presents three example resilience measurement scenarios that describe a context of related process areas (referred to as ecosystems) and the derivation of a measure that supports each of these: one for managing risk, one for managing incidents, and one for protecting information assets. This section also presents several suggested updates to the measures that appear as elaborations in selected CERT-RMM v1.0 process areas that arose from the analysis of the scenarios from a measurement perspective [Caralli 2010b].

The report closes with a brief description of sources that can be used in helping define a measurement program and process and by identifying next steps and future directions for this research project.

Figure 1 provides a roadmap for and brief description of each section of this report.

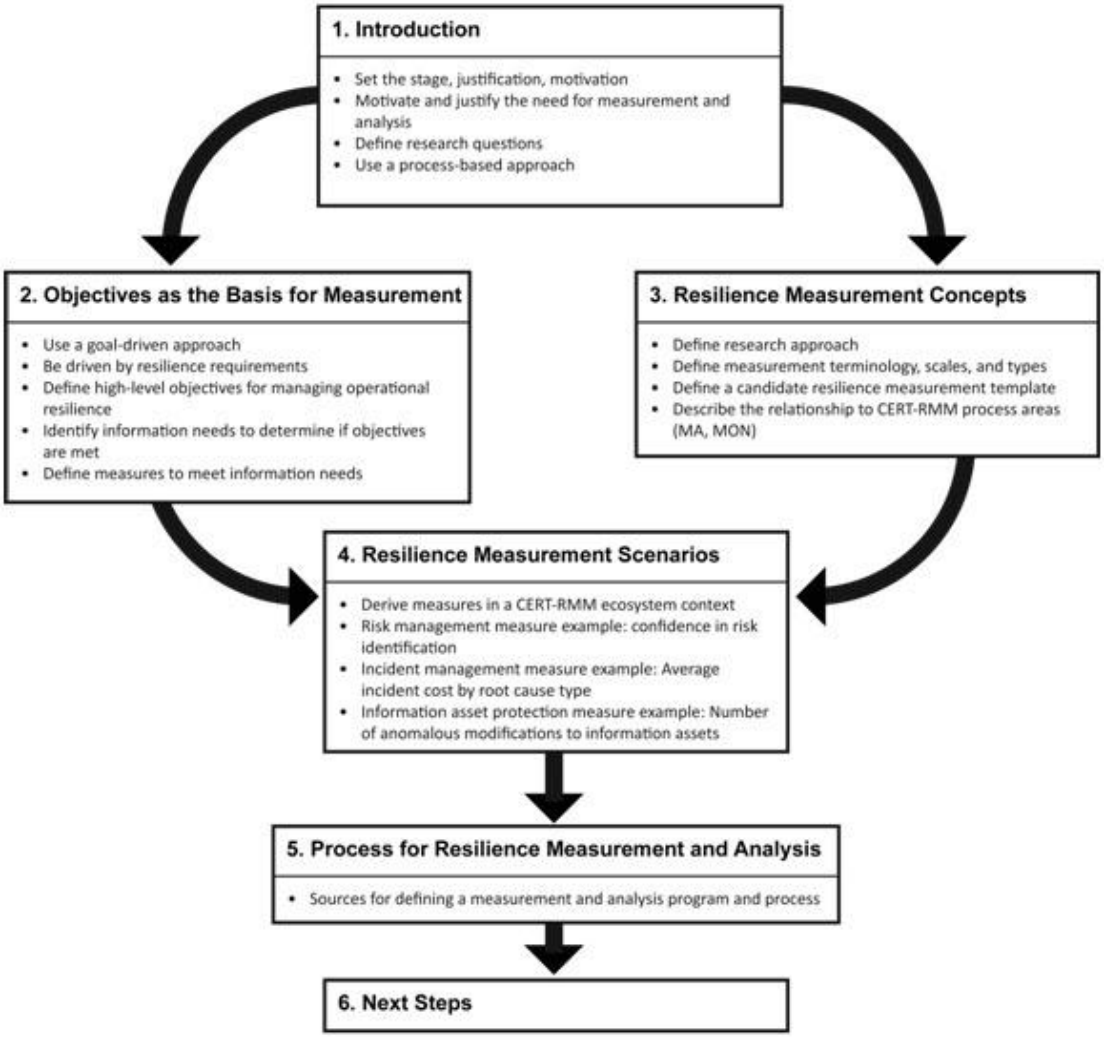


Figure 1: Report Overview

2 Establishing Objectives as the Basis for Measurement

2.1 Introduction

Many organizations measure just for the sake of measuring, with minimal thought given as to what purpose and business objectives are being satisfied by measuring – and what questions any given measure is intended to inform. This approach focuses too much on what to measure and how to measure, and not nearly enough on why the measure is needed. One common approach is to identify a standard or code of practice (such as ISO 27002 [ISO 2005]) and then measure the implementation and performance of practices contained in the standard. This checklist-based approach is typically used in support of compliance activities. The *CERT Resiliency Engineering Framework* (previous name for CERT-RMM) *Code of Practice Crosswalk* [REF Team 2008] contains a list of standards and codes of practice that are commonly used for this purpose. In fact, the example measures associated with each CERT-RMM process area (PA) could be used in this way (measurement as a compliance-driven activity), but they are more effectively used based on an objective-driven approach. Measurement can be costly so organizations need to ensure that they are collecting, analyzing, and reporting the right measures to inform the right decisions at the right time, driven by business and mission objectives.

Our measurement and analysis research project uses an objective-driven approach based on a variation of the Goal Question (Indicator) Metric (GQ(I)M) Method developed at the SEI [Park 1996]. GQ(I)M draws upon earlier work done by Basilli and Rombach in defining the Goal Question Metric (GQM) method [Basili 1984, 1988, 1994], [Rombach 1989]. For both of these approaches and for goal-driven measurement in general, the primary question is not "What measures should I use?" but "What do I want to know or learn?" [SEMA 2010]

A goal-driven approach is based upon the assumption that for an organization to measure in a meaningful way, it must

1. Determine business goals (objectives)[7] or a key question to be answered.
2. Determine the information needs necessary to determine if the objective is met or to answer the question.
3. Quantify the information needs whenever possible (in the form of measures).
4. Analyze measures to determine whether the goals and objectives were achieved or if the question was adequately answered.

Using this method, we first define a set of high-level objectives for the management of operational resilience from which information needs, measurement objectives, and measures can be derived.

[7] For the purpose of this report, we use the term goal and objective interchangeably, defined as “the end toward which effort is directed.” http://www.merriam-webster.com/.

The purpose of defining high-level objectives for managing operational resilience is to ensure that all resilience measures derive from business objectives for operational resilience. We need to ensure that all resilience measures that we define (and invest in collecting, analyzing, and reporting) have a direct link to one or more of these objectives. Lower-level measures should indirectly link by mapping to a directly linked measure. We also need to ensure that measures provide the information that is needed to manage the operational resilience management (ORM) program and evaluate its performance. We anticipate that the degree or extent of linkage to high-level objectives may help establish measurement priorities in the large (as contrasted with measurement priorities for a specific CERT-RMM PA or set of PAs). We fully expect that the measurement of these high-level objectives will involve goals and practices from the 26 process areas of the CERT-RMM.

Objectives for managing operational resilience (and thus the measurement and analysis of operational resilience) derive from resilience requirements (refer to the Resilience Requirements Definition (RRD) process area). As described in the *CERT Resilience Management Model Version 1.0,* an operational resilience requirement is a constraint that the organization places on the productive capability of a high-value asset to ensure that it remains viable and sustainable when charged into production to support a high-value service [Caralli 2010a]. In practice, operational resilience requirements are a derivation of the traditionally described security objectives of confidentiality, integrity, and availability. Well known as descriptive properties of information assets, these objectives can also be applied to other types of assets (people, technology, and facilities) that are of concern when managing operational resilience. Resilience requirements provide the foundation for protecting assets from threats and making them sustainable so that they can perform as intended in support of services. Resilience requirements become a part of an asset's DNA (just like its definition, owner, and value) that transcend departmental and organizational boundaries because they stay with the asset regardless of where it is deployed or operated.

Resilience requirements are at the heart of the operational resilience management program. To develop complete resilience requirements, the organization considers not just specific asset-level requirements but organizational drivers (e.g., strategic goals and objectives and critical success factors), risk appetite, and risk tolerances.[8] As shown in Figure 2, organizational drivers provide the rationale for investing in resilience activities, and risk appetite and tolerances provide parameters for prioritizing risk mitigation actions. Organizational drivers are also important because they enable the identification of the organization's high-value services. High-value services are critical in achieving the organization's mission and should be the focus of the organization's operational resilience management activities and resources.

Resilience requirements form the basis for protection and sustainment strategies. These strategies determine the type and level of controls needed to ensure the operational resilience of high-value services and their associated assets (i.e., controls that protect services and assets from disruption as much as possible and that sustain services and assets in the event of disruption). Conversely, controls must satisfy the requirements from which they are derived. Aligning control objectives with resilience requirements can help the organization to avoid deploying an extensive number of overlapping and redundant controls.[9]

---

[8] Refer to the Resilience Requirement Development (RRD) and Risk Management (RISK) PAs.

[9] Refer to the Controls Management (CTRL) PA.

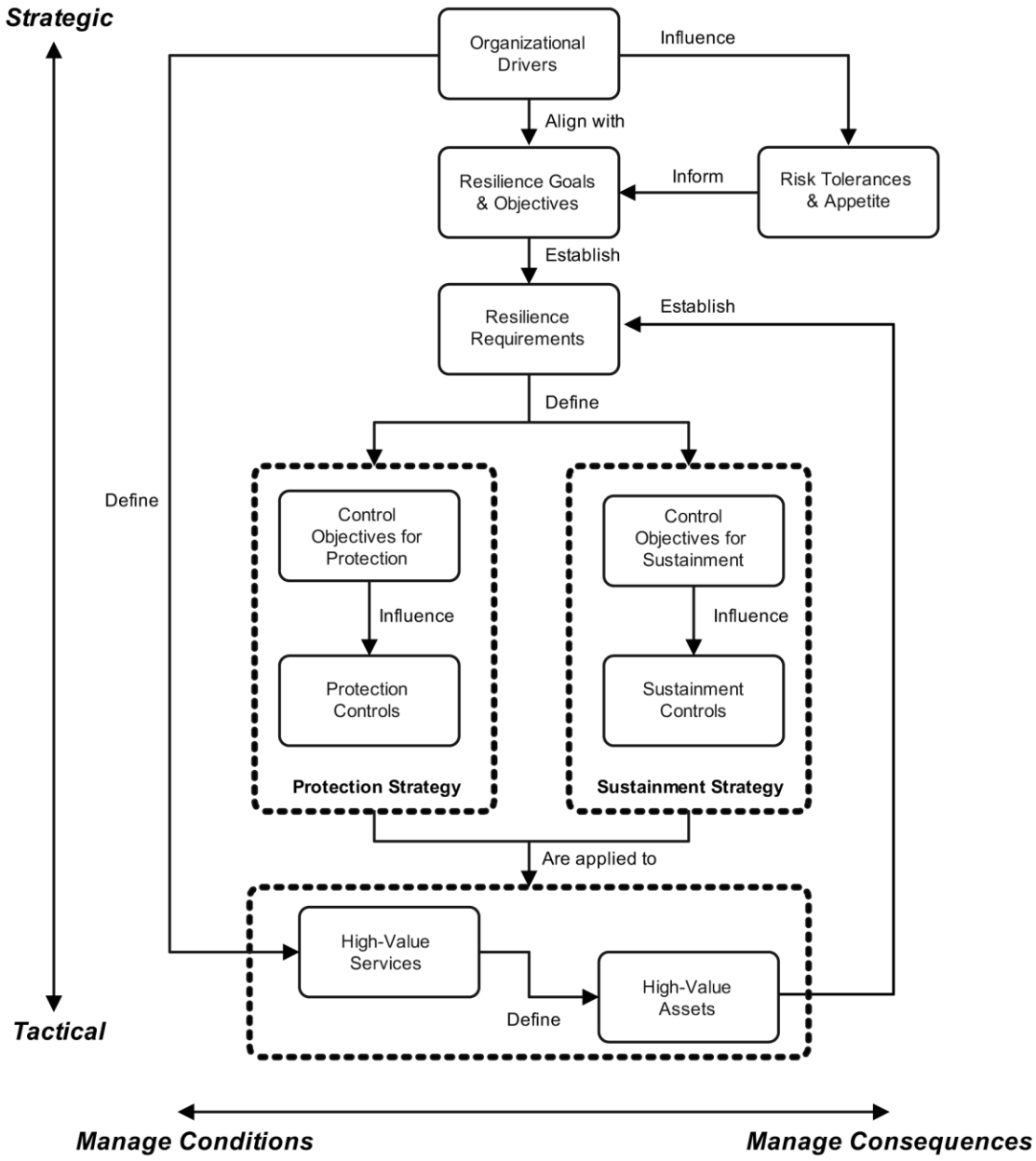


Figure 2: Resilience Requirements Establish the Foundation for Resilience Measurement

2.2 Objectives for Managing Operational Resilience

The objectives for an ORM program serve as the basis or foundation for resilience measurement and analysis. Defining, collecting, analyzing, and reporting measures that do not have a direct connection to a specific organization purpose, objective, or key question waste precious organizational resources and the time and attention of business leaders and other key stakeholders who depend on measures to inform decisions. Based on Figure 2 and its use in [Caralli 2010a], we define the following six statements as the high-level objectives for managing an ORM program. These may be interpreted and tailored for a specific organization as the basis for its operational resilience and measurement program.

The ORM program

- O1: derives its authority from and directly traces to organizational drivers[10]
- O2: satisfies enterprise resilience requirements that are assigned to high-value services and their associated assets[11]
- O3: satisfies high-value asset resilience requirements
- O4: via the internal control system, ensures that controls for protecting and sustaining high-value services and their associated assets operate as intended
- O5: manages (identifies, analyzes, mitigates) operational risks to high-value assets that could adversely affect the operation and delivery of high-value services
- O6: in the face of realized risk, ensures the continuity of essential operations of high-value services and their associated assets

Each objective has a unique identifier to aid in traceability. Measures for managing operational resilience and determining resilience performance will be based on these objectives, and are used in the examples presented throughout this report. The CERT-RMM PAs that inform and elaborate each objective is shown in Tables 1 through 6.

2.3 Deriving Meaningful Measures from Objectives: an Illustration

The need for meaningful measures is derived from and can be directly traced to some objective, purpose, or key question. The purpose of this section is to illustrate how meaningful measures for managing operational resilience can be derived from high-level objectives. We apply the SEI's GQ(I)M method [Park 1996] that is further described in Section 3.2 as a foundational measurement concept. We illustrate its use at this point in the report to further elaborate and define the six ORM program objectives. (Additional examples of this derivation process within the context of specific CERT-RMM process areas are included in Section 4).

We have used the following process to derive measures of interest from an objective or question:

1. Information Needs: Examine the objective (or question) and determine what information would be needed to assess the extent to which the objective is (or is not) being met.

2. Measurement Objective[12]: Identify one or more measurement objectives which would satisfy the information need.

3. Measures: Identify a short list of candidate measures to meet each measurement objective. These can then be further described in a measurement template along with a range of interpretations (refer to Section 3.3).

---

[10] An alternative way of stating this might be "The ORM Program derives its authority from a directive given by a senior, high-level executive." This could be considered one form of organizational driver.

[11] An alternative way of stating this might be "The ORM program satisfies governance, compliance, policy, framework, assessment, and reporting requirements." These could all be considered expressions of enterprise resilience requirements.

[12] While it reflects the operational resilience objective, the measurement objective is typically stated more precisely.

The tables that follow apply this three-step process to each of the six high-level objectives for managing operational resilience. During this process, we define each of the objectives and demonstrate how to derive meaningful measures for them. Readers need to have working knowledge of CERT-RMM v1.0 and its concepts and terminology to fully understand these descriptions. Where applicable, traceability to the relevant CERT-RMM process areas, specific goals, and specific practices is provided. EF.SG1.SP1 is shorthand for Specific Practice 1 (SP1) of Specific Goal 1 (SG1) of the Enterprise Focus (EF) Process Area of the CERT-RMM. For a list of the twenty six process areas of the CERT-RMM, refer to the Acronyms section of this report.

Table 1: Objective O1 – The ORM program derives its authority from and directly traces to organizational drivers.

Step	**Description**	**CERT-RMM Traceability**
1. Information Needs	Documented organizational drivers Traceability of strategic resilience objectives to organizational drivers (strategic objectives and critical success factors)	EF:SG1.SP1; EF:SG1, SP2
	Documented ORM program activities	EF:SG2.SP1; EF:SG2.SP2
	Traceability of the ORM program activities to organizational drivers Traceability of CERT-RMM process areas (goals, practices) to organizational drivers	
2. Measurement Objective	Demonstrate that the ORM program directly supports organizational drivers.	
3. Measures	Number of ORM program activities that *do not* directly support organizational drivers	
	Number of CERT-RMM PAs that *do not* directly support organizational drivers	
	Extent to which an organizational driver *cannot* be satisfied without one or more ORM program activities (or one or more CERT-RMM PAs) Conversely, for each ORM program activity (or CERT-RMM PA), number of organizational drivers that require it (goal is = or >1)	

Table 2: Objective O2 – The ORM program satisfies enterprise resilience requirements that are assigned to high-value services and their associated assets

Step	**Description**	**CERT-RMM Traceability**
1. Information Needs	Documented enterprise resilience requirements	RRD:SG1.SP1
	Documented high-value services	EF:SG1.SP3; SC:SG2.SP1
	Traceability of enterprise resilience requirements to high-value services	RRD:SG2.SP2
	Confirmation that enterprise resilience requirements (and corresponding traceability) are up to date (reflect all changes)	RRM:SG1.SP3
	Evidence that each high-value service satisfies the enterprise resilience requirements that have been assigned to it and to its associated assets. Such evidence is produced periodically and on demand throughout the service lifecycle.	RRD:SG2.SP2; asset-specific PAs (KIM:SG2.SP1, TM:SG2.SP1, EC:SG2.SP1, PM:SG3); CTRL:SG4.SP1; SC:SG4.SP1; MON

2. Measurement Objective	Demonstrate that the ORM program satisfies all enterprise resilience requirements that are allocated to high-value services and associated assets	
3. Measures	Number of enterprise resilience requirements	RRD:SG1.SP1
	Number of high-value services	EF:SG1.SP3; SC:SG2.SP1
	Number of high-value assets by asset category	EC:SG1; KIM:SG1; PM:SG1; TM:SG1
	Traceability of high-value services to associated assets	ADM:SG2
	Percentage of enterprise resilience requirements that are (*are not*) assigned to (intended to be satisfied by) high-value services and associated assets	RRD:SG2.SP2
	Percentage of high-value services and associated assets that *do not* satisfy their allocated enterprise resilience requirements	RRD:SG3; RRM; EC; KIM; PM; TM; MON

Table 3: Objective O3 – The ORM program satisfies high-value asset resilience requirements[13]

Step	**Description**	**CERT-RMM Traceability**
1. Information Needs	Documented high-value assets	EC:SG1.SP1;KIM:SG1.SP1;TM:SG1.SP1;PM:SG1.SP1
	Documented asset resilience requirements	RRD:SG2.SP1 RRD:SG2.SP2 KIM:SG2.SP1; EC:SG2.SP1; PM:SG3; TM:SG2.SP1
	Asset to service and service to asset traceability	ADM:SG2. SP1 ADM:SG2.SP2 RRD:SG2.SP1
	Mapping of asset resilience requirements to high-value services (which constitute the resilience requirements for the service)	RRD: SG2.SP1
	Confirmation that asset resilience requirements (and corresponding mapping) are up to date (reflect all changes)	RRM:SG1.SP3
	Evidence that each high-value asset satisfies the resilience requirements that have been assigned to it. Such evidence is produced periodically and on demand throughout the service lifecycle.	RRD:SG2.SP1; asset-specific PAs (KIM:SG2.SP1, TM:SG2.SP1, EC:SG2.SP1, PM:SG3); CTRL:SG4.SP1 MON
2. Measurement Objective	Demonstrate that the ORM program satisfies all resilience requirements that are assigned to high-value assets	
3. Measures	Number of asset resilience requirements[14]	RRD:SG2.SP1
	Percentage of asset resilience requirements that have been (have not been) assigned to one or more assets	RRD:SG2.SP1
	Percentage of high-value assets that do not have assigned resilience requirements	RRD:SG2.SP1
	Percentage of asset resilience requirements that have been (have not been) mapped to high-value services	RRD:SG2.SP1
	Percentage of high-value assets that do not satisfy their assigned resilience requirements	RRD:SG3; RRM; EC; KIM; PM; TM; MON

[13] Services must implement strategies for protecting and sustaining assets that ensure asset resilience requirements continue to be met when assets are used or deployed in support of a service. In other words, services inherit the resilience requirements from the assets that support them.

[14] Likely broken out by asset type, service, or some other meaningful category

Table 4: Objective O4 – The ORM program, via the internal control system, ensures that controls for protecting and sustaining high-value services and their associated assets operate as intended.

Step	Description	CERT-RMM Traceability
1. Information Needs	Documented asset profiles Documented service profiles	ADM:SG1.SP2 EF:SG1.SP3
	Control objectives	CTRL:SG1
	Traceability between control objectives and controls	CTRL:SG2.SP1
	Protection controls for assets Protection controls for services	CTRL:SG2.SP1 EC:SG2.SP2, KIM:SG2.SP2, PM: all SGs/SPs TM:SG2.SP2
	Sustainment controls for assets Sustainment controls for services	EC: SG4 KIM: SG4, SG5, SG6 PM:SG2.SP2, SG3 TM:SG5 SC: all SGs/SPs
	Control assessment results	CTRL:SG4
2. Measurement Objective	Demonstrate that the ORM program (1) satisfies control objectives and (2) implements controls that protect and sustain high-value services and their associated assets.	
3. Measures	Percentage of control objectives that are satisfied (not satisfied) by controls (enterprise-level, by service, by asset category)	CTRL;SG3
	Percentage of high-value assets for which there are no (missing) protection (sustainment) controls (by asset category)	CTRL:SG4 asset-specific PAs referenced above
	Percentage of high-value services for which there are no (missing) protection(sustainment) controls	CTRL:SG4 SC
	Percentage of high-value asset controls (protect, sustain) that are ineffective or inadequate (by asset category) as demonstrated by: • unsatisfied control objectives • unmet resilience requirements • outstanding control assessment problem areas above established thresholds/without remediation plans	asset-specific PAs referenced above CTRL:SG4
	Percentage of high-value service controls (protect, sustain) that are ineffective or inadequate (by service, by associated asset) as demonstrated by: • unsatisfied control objectives • unmet resilience requirements • outstanding control assessment problem areas above established thresholds/without remediation plans	asset-specific PAs referenced above CTRL:SG4 SC

Table 5: Objective O5 – The ORM program manages (identifies, analyzes, mitigates) operational risks to high-value assets that could adversely affect the operation and delivery of high-value services.

Step	Description	CERT-RMM Traceability
1. Information Needs	Sources and categories of risk	RISK:SG1.SP1
	Asset to service and service to asset traceability	ADM:SG2. SP1 ADM:SG2.SP2 RRD:SG2.SP1
	Identification of high-value assets and high-value services	ADM:SG1.SP1 EF:SG1.SP3 EC:SG1.SP1;KIM:SG1.SP1; TM:SG1.SP1;PM:SG1.SP1
	List of operational risks (by asset category and service) with prioritization, impact valuation, risk disposition, mitigations, and current status	RISK:SG3.SP1; SG3.SP2; SG4.SP2; SG4:SP3; SG5.SP2
	Categorization of operational risks (by asset category and service) by disposition (avoid, accept, monitor, research or defer, transfer, mitigate or control)	RISK:SG4.SP3
2. Measurement Objective	Demonstrate that the ORM program effectively manages risks to high-value services and their associated assets.	
3. Measures	Confidence factor (likelihood; high, medium, low) that all risks that need to be identified have been identified	
	Number and percentage of risks with a "mitigate or control" disposition without mitigation plans	RISK:SG4.SP3 RISK:SG5.SP1
	Number and percentage of risks with a "mitigate or control" disposition with mitigations that are not yet started and in-progress (vs. completely implemented)	RISK:SG4.SP3 RISK:SG5.SP2
	Extent to which current risks with a "mitigate or control" disposition are effectively mitigated by their mitigation plans	RISK:SG6
	Elapsed time since risks with the following dispositions were last reviewed and disposition confirmed: avoid, accept, monitor, research or defer, transfer	RISK:SG6

Table 6: Objective O6 – In the face of realized risk, the ORM program ensures the continuity of essential operations of high-value services and their associated assets.

Step	Description	CERT-RMM Traceability
1. Information Needs	Description of incident, disaster, or other disruptive event (realized risk) including affected high-value services and their associated assets	IMC:SG3 SC:SG6
	List of high-value services and associated assets affected by the disruption	
	Service continuity plans for disrupted services	SC:SG3.SP2
	Results of executing service continuity plans for disrupted services	SC: SG6.SP1; SG6.SP2
2. Measurement Objective	Demonstrate that the ORM program sustains high-value services and associated assets during and following a disruptive event.	

3. Measures	Number and percentage of disrupted, high-value services without a service continuity plan	
	For disrupted, high-value services with a service continuity plan, percentage of services that delivered (that did *not* deliver) service as intended throughout the disruptive event	
	For disrupted, high-value services with *no* service continuity plan, percentage of services that delivered (that did *not* deliver) service as intended throughout the disruptive event. One way of stating these as measures of probability include: • probability of delivered service thru a disruption event • conditional probability of a disrupted high value service given no service continuity plan • conditional probability of a disrupted high value service not delivering intended service given no service continuity plan	

Appendix 1 contains some suggested, additional questions that can be used to help determine an organization's current and desired state of operational resilience and thus drive the selection and definition of measures to aid in making well informed investment decisions.

3 Resilience Measurement Concepts

This section describes the core measurement concepts that are used to address the research questions for the resilience measurement and analysis research project. It also defines a candidate measurement template, which is then applied in Section 4.

From its inception, measurement has been an integral part of the CERT-RMM [Caralli 2010a]. Elaborations in the model include examples of measures for each process area. Most of the measurement examples can be found in the Generic Goals section of each process area; specifically, Generic Goal 2 Generic Practice 8 (GG2.GP8), "Monitor and Control the Process." The measurement examples in the CERT-RMM are based on expert judgment and from observed in-use measures.

As we started to formalize a measurement approach for operational resiliency, our first task was to study and understand the sample measures defined in the CERT-RMM. Based on our understanding of the sample measures, we agreed on the following:

1. We chose the word "measurement" (and its companion noun "measure") instead of "metrics" for our work. The reason for this was simple: there seem to be many definitions of the word "metric," with very different meanings. Examples include a "metric function," or the "metric system," or even the study of "meter" or rhythm in poetry. On the other hand, the definition of measurement as mapping from the real world to a system of numbers and symbols is more universally accepted as indicated in these definitions:

   Measurement: the assignment of numerals to objects or events according to [a] rule [Stevens 1959].

   Measurement: the process by which numbers or symbols are assigned to attributes of entities in the real world in such a way as to characterize the attributes by clearly defined rules [Fenton 1991, Fenton 1995].

2. Choosing the words "measurement" and "measure" allowed us to use concepts from an entire body of foundational knowledge and research and provided a solid foundation for measurement in the operational resilience domain [Stevens 1946, 1951], [Krantz 1971], [Roberts 1979], [Ghiselli 1981], [Wheeler 2000], and [Hubbard 2007].

3. The CERT-RMM addresses operational resilience for information security management, business continuity management, and aspects of IT operations management. Also, the pedigree of the CERT-RMM can be traced back to the Capability Maturity Model Integration [CMMI Product Team 2006]. Effective measurement practices from all of these domains influenced our approach to measurement for operational resilience.

The considerations above led to the following research approach:

- Survey existing codes of practice for the three constituent domains of the CERT-RMM (information security, IT operations, business continuity), focusing on measurement, specifically [ITGI 2007], [BSI 2006], [ISO 2005], [DRJ 2006], [FFIEC 2008], and [REF Team 2008].

- Survey measurement frameworks used in related disciplines (software development, software security, and software assurance – the SEI's core competence). In particular, we looked at the Capability Maturity Model Integration (CMMI) [CMMI Product Team 2006], the SEI Software Engineering Measurement and Analysis work [SEMA 2010], the Practical Software and Systems Measurement work [PSM 2010], the System Security Engineering Capability Maturity Model [SSE-CMM 2003], National Institute of Standards and Technology (NIST) Special Publication 800-55 *Performance Measurement Guide for Information Security* [NIST 2008], U.S. Department of Homeland Security Software Assurance Measurement Working Group reports including the Practical Measurement for Software Assurance [Bartol 2008], the Building Security In Maturity Model [McGraw 2010], and others.
- Formulate core resilience measurement concepts, based on established measurement foundational knowledge, described in Sections 3.1 and 3.2.
- Validate concepts against the existing sample measures in CERT-RMM in the generic goals section GG2.GP8. An example is shown in Table 20.
- Formulate a candidate measurement framework including a template for defining measures, described in Section 3.3.
- Exercise the framework against ORM objectives for several example areas of interest, described in Section 4.
- Validate the framework against the two process areas in the CERT-RMM that focus most heavily on measurement: the Measurement and Analysis (MA) and the Monitoring (MON) process areas, described in Sections 3.3.1and 3.3.2.

3.1 Measurement Relationships and Definitions

An organization may have varied needs for resilience-related information. For example, these needs could be to determine status, to assess risk, or to predict and prepare for future events; they are dependent on the organization's resilience goals. In the CERT-RMM, measurement is performed to satisfy a need for resiliency-related information. To define a measurement framework, the connection from information needed to attributes measured must be determined. Figure 3 shows a graphical representation of this connection[15] [Park 1996], [Mills 1988]. Although the need for information is usually driven from the top down, measures are collected by quantifying the attributes of assets, services, and processes.

[15] Based on concepts in ISO/IEC 15939 Systems and software engineering – Measurement process [ISO 2007].

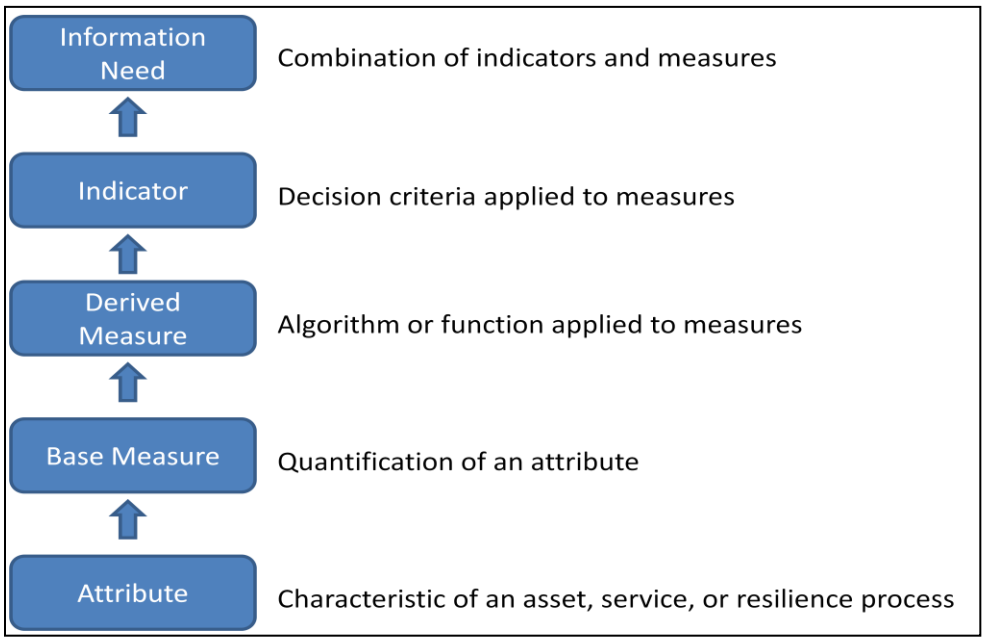


Figure 3: Resilience Measurement Relationships

Attribute

An attribute is a property, trait, or characteristic of an asset, service, or resilience process. A person's attributes may include height, weight, or eye color. An asset's attributes may include its cost or value. Process attributes include elapsed time and time in phase. Service attributes include response time and service failures.

Base Measure

A measure quantifies an attribute. A person's height can be measured in feet and inches, service response time can be measured in seconds or minutes, and process elapsed time could be measured in days or months.

A base measure is a directly observable attribute of an asset, service, or resilience process. A base measure is functionally independent of other measures and is defined by fundamental units that are not composed of any other units.

The most frequent base measures in CERT-RMM are defined in Table 7.

Table 7: Most Frequent CERT-RMM Base Measures

Base Measure	Description	Question Answered	Examples
Count	A measure of the number of an entity	How many?	number of high-value assets by asset category number of requirements number of incidents
Cost or effort	Cost is a measure of the value of money, while effort is a measure of the number of labor units, usually expressed as person hours, person days, or person weeks.	How much?	cost of acquiring a high-value asset effort spent in developing a resilience requirements definition process effort required to address training gaps for vital staff

Schedule	A measure of a calendar period, usually expressed as days, weeks, month or years.	When? How Long?	schedule for implementing controls schedule for completing required training schedule for developing a risk management process
Defects	An error, flaw, failure, or fault in a resilience process, service, or asset	How well?	In CERT-RMM, defects lead to service continuity test failures vulnerabilities introduced during Resilient Technical Solution Engineering (RTSE) process activities incidents resulting from exploited vulnerabilities

Derived Measures

A derived measure is a mathematical function of two or more base and/or derived measures. Examples of resilience derived measures include percentage of redundant controls, rate of change of resource needs to support the resilience requirements development process, and percentage of software assets for which the cost of compromise (loss, damage, disclosure, disruption in access to) has been quantified.

Indicators

An indicator is typically a graphical or tabular display of one or more measures, with corresponding guidance for interpreting the information being displayed. Indicators are important because a "picture is worth a thousand words" and deciding how to communicate information can sometimes help decide which attributes to measure.

An indicator has one or more of the following characteristics:

- Indicators are almost always derived measures.
- Indicators are designed to communicate so as to fulfill specific information needs.
- Indicators frequently present comparisons between two values, such as planned and actual values.

Information Need

An enterprise has information needs at many levels: from the senior executive who needs to make a strategic decision that may impact the entire organization for years to come, to the service operator who needs to make a tactical decision about the next step to perform. Information needs fall into the following five broad categories, derived from measurement work in the software engineering domain: [SEMA 2010, Park 1996]

1. characterize: gain understanding of assets, services, and resilience processes
2. evaluate: determine current status with respect to plans
3. predict: determine future state based on current status and historical data
4. improve: identify cost, schedule, quality, and other performance problems
5. benchmark: compare with industry or enterprise best practices

3.1.1 Subjective and Objective Measures

Measures can be subjective or objective. With a subjective measure, different qualified observers can identify different values for the measure. An objective measure is one where multiple qualified observers who determine identical results for a given measure.

For example, elapsed time between two defined events is usually an objective measure, while competence of a system administrator is usually a subjective measure. Objective measures are repeatable; subjective measures often are not. This does not mean that subjective measures are not useful: patient judgment of pain levels and employee responses to an opinion survey are examples of useful subjective measures.

3.1.2 Scales for Resilience Measures

Measurement scales define the characteristics and types of values that can be assigned to a measure. They are useful for collecting, analyzing, and interpreting data as it pertains to the measure. Four basic scales are commonly recognized: nominal, ordinal, interval, and ratio [Park 1996], [Mills 1988]. The assignment and application of these scales is often left undefined initially but help to determine appropriate statistical analysis that could be performed with a measure.

Table 8 provides a definition and several CERT-RMM examples for each measurement scale.

Table 8: Measurement Scales

Scale	Possible Mathematical Operations	Definition and Examples
Nominal (subjective or objective)	=, ≠	**Definition**: Unordered/unranked values or categories. **CERT-RMM example**: Type of service, for example, a CRM service, an HR service, or a payroll service (the only operation allowed is to determine if one service is the same as or is different than another service).
Ordinal (subjective or objective)	<, >	**Definition**: Ranked/ordered values or categories. Differences in values are not necessarily meaningful. **CERT-RMM example**: Should allow comparative assessment, such as the experience level of a security professional: high, medium, low
Interval (usually objective)	+, -, /, *	**Definition**: Ordered values with intervals of equal meaning. A difference in values can be meaningful but there is no absolute zero. **CERT-RMM example**: Start-date and end-date for an asset used or deployed in support of a service.
Ratio (usually objective)	+, -, /, *	**Definition**: Ordered values with intervals of equal meaning and a concept of absolute zero. **CERT-RMM example**: Number of assets used by a service (100 assets are twice as many as 50 assets and 0 assets is a valid quantity of assets).

A *nominal* scale assigns a label to an attribute, usually by placing it in some sort of category. The mathematical structure that represents a nominal scale most closely is an unordered set. An example includes a person's eye color: green, blue, or brown. Valid operations for this scale include counts, equivalence, and set membership. The central tendency is defined by the arithmetic mode operation. Median and mean are not valid operations for a nominal scale. For example, it makes

sense to say that brown eye color occurs most frequently (mode) but not that the average eye color is green.

An *ordinal* scale allows measured results to be ranked or placed in ascending or descending order. However, differences between values may have no meaning. An example of an ordinal measure is the capability level of a CERT-RMM process area: the level can vary from level 1 to level 3. We know that level 3 is better than level 1, but we cannot make any judgments about level 3 being 3-times better than level 1, or that the difference between level 3 and level 2 is the same as the difference between level 2 and level 1. The central tendency of an ordinal scale can be the mode or the median. However, mean is not a valid operation. For example, it makes no sense to say that the average capability level of a CERT-RMM process area is 2.5.

An *interval* scale can be ranked and allows for meaningful differences among values. However, there is no concept of an absolute "zero." A common example is measuring temperature with the Celsius scale, where the unit of measurement is 1/100 of the difference between the boiling temperature and the freezing temperature of water at atmospheric pressure. Difference calculations are valid, but ratios are not. Let us say that the temperature in the morning was 60ºF, and the afternoon was 80ºF. It is meaningful to say that the difference in temperatures was 20ºF. We can even say that the average afternoon temperature has been 78 ºF, but saying that the afternoon temperature was a third higher than the morning temperature makes no sense. The central tendency of this scale can be mode, median, or mean.

A *ratio* scale adds a meaningful absolute zero value, which leads to performance of all mathematical operations including addition, subtraction, multiplication, division, and ratios. Examples of measures include cost, service response time, and number and percentage of service continuity test failures.

3.1.3 Resilience Measurement Types

The CERT-RMM reflects three types of measures: implementation, effectiveness, and process performance.

Implementation measures help to answer the question: Is this process or practice being performed? Implementation measures help with compliance assessments but make no judgment about how well the practice is being performed. These measures are associated with lower capability levels: levels 1 and 2, for example. This type of measure would be typical in organizations starting a resilience improvement effort using CERT-RMM. Sample implementation measures for Resilience Requirements Development (RRD) process area include:

- number of services and assets for which requirements have been defined and documented
- number of services and assets for which there are no stated requirements or that have incomplete requirements
- percentage of asset owners participating in the development of requirements

Effectiveness measures help to answer the question: How good is the output or outcome of the practice being performed? Outcome-related measures help determine the effectiveness of the process or practice that produces the outcome. These measures are usually associated with higher

capability levels: level 3 and higher[16]. Sample effectiveness measures for the RRD process area include:

- number of service continuity test failures resulting from incomplete resilience requirements
- number of compliance audit failures resulting from problems with the resilience requirements
- number of violations of the confidentiality, integrity, and availability qualities or properties of an asset or service resulting from problems with the resilience requirements developed for that asset or service

These 3 effectiveness measures could also be stated as probabilities, conveying the extent to which a service continuity test failure, for example, is likely to result from incomplete resilience requirements in advance of an actual test failure.

Process performance measures help to plan, predict, and control the process, which lead to the ability to manage and improve the process. These measures are also associated with higher levels of capability: level 3 and higher. Sample process performance measures for the RRD PA help answer questions such as:

- What is the cost of performing the RRD process?
- Are costs to perform the RRD process declining?
- How predictable is the RRD process in terms of plan vs. actual costs and schedule?
- Are RRD process cost and schedule estimation errors improving?

3.2 Goal Question (Indicator) Measure

According to management guru Peter Drucker, *"The most serious mistakes are not being made as a result of wrong answers. The truly dangerous thing is asking the wrong question."*[17] How do you know what question(s) to ask to meet the information needs of an ORM objective? We have found that replacing the term "business goal" with "resilience goal" makes the method applicable to measuring operational resilience. We will not cover GQ(I)M methods in detail here. Instead, we guide the reader to references for detailed information.

Basilli and Rombach defined the Goal Question Metric (GQM) method. The GQM approach is based upon the assumption that for an organization to measure in a meaningful way, it must

1. determine business goals
2. determine information needs
3. quantify the information needs whenever possible
4. analyze the quantified information to determine whether the goals were achieved [Basili 1984, 1988, 1994], [Rombach 1989]

[16] CERT-RMM v1.0 includes capability levels up to level 3. The CERT-RMM development team plans to explore the value and definition of higher levels of capability in the future.

[17] http://www.leadershipnow.com/probsolvingquotes.html

Park, et. al. expanded on the GQM method to develop the Goal Question (Indicator) Measure (GQIM) method. The following ten-step process leads from a business goal to a plan for implementing the measures required to support the goal [Park 1996]:

1. Identify business goals.
2. Identify knowledge and learning goals.
3. Identify sub-goals.
4. Identify the entities and attributes related to sub-goals.
5. Formalize measurement goals.
6. Identify quantifiable questions and the related indicators that will help to achieve measurement goals.
7. Identify the data elements to collect that will be used to construct the indicators that help answer the questions.
8. Define the measures to be used and make these definitions operational.
9. Identify the actions to take to implement the measures.
10. Prepare a plan for implementing the measures.

The resilience measurement template defined in the next section can be used to record the outputs of the GQ(I)M method.

3.3 Resilience Measurement Template

Measurement templates help to organize the goals, attributes, and measures that an organization needs to define as it begins to implement an operational resilience measurement program. A template establishes a pattern and serves as a guide, helps connect resilience goals to the appropriate attributes, and provides repeatability in collecting, analyzing, and reporting measures. Templates also help to answer the basics for information gathering and information presentation: who, what, where, when, why, and how.

1. Who is the measure for? Who are the stakeholders? Who collects the data/information that is the source for the measure?
2. What is being measured?
3. Where is the data/information stored?
4. When/how frequently are the measures collected?
5. Why is this measure important?
6. How are the data collected? How is the measure presented? How is the measure used?

Another way of thinking about measurement templates is in terms of operational definitions. According to Deming, an operational definition gives communicable meaning to a concept by

specifying how the concept is measured and applied within a particular set of circumstances [Deming 1986]. Without an operational definition, measures can be misunderstood. The following example illustrates the need for operational definitions. Suppose you were asked the following question: Is this table clean? The answer would depend on the operational definition of the measure "cleanliness." If the table is being used as a worktable, then lack of clutter could mean it is clean. If the table is being used as a dining table, then wiping it clean with a detergent may be needed. However, if surgical instruments are to be placed on a table, then it may need to be wiped clean with antiseptics. A measurement template helps capture the operational definition.

There are two sample measurement templates shown in this section: Table 9 shows a base measure template and Table 10 shows an indicator template. The base measure template provides guidance for collecting base measures. The indicator template helps organizations use base and/or derived measures to provide information about a resilience objective. The templates borrow heavily from the NIST *Performance Measurement Guide for Information Security* [NIST 2008] and from the SEI Indicator Template [Goethert 2001].

The templates are meant to be used as a point of departure; organizations are encouraged to tailor these to suit their needs. Alternatively, organizations may choose to develop their own templates.

Table 9: Base Measure Template

Measure Name/ID	Name or ID of base measure
Measurement Description	Describe the attribute being measured, for example, number of resilience requirements for a service.
Measurement Scale	1. Define the possible set of values, or identify the categories, that are valid for the measure: for example, positive whole numbers only. 2. Define the type of scale: nominal, ordinal, interval, or ratio 3. Define the units
Data Collection **How** **When/How Often** **By Whom**	Describe how the data will be collected (process), when and how often the data will be collected (event driven, periodic), and who will collect the data (people, tool). Specify if collection method is objective or subjective. Refer to forms or standards if needed.
Data Storage **Where** **How** **Access Control**	Identify where the data is to be stored. Identify the storage media, procedures, and tools for configuration control. Specify how access to this data is controlled.

Table 10: Indicator Template

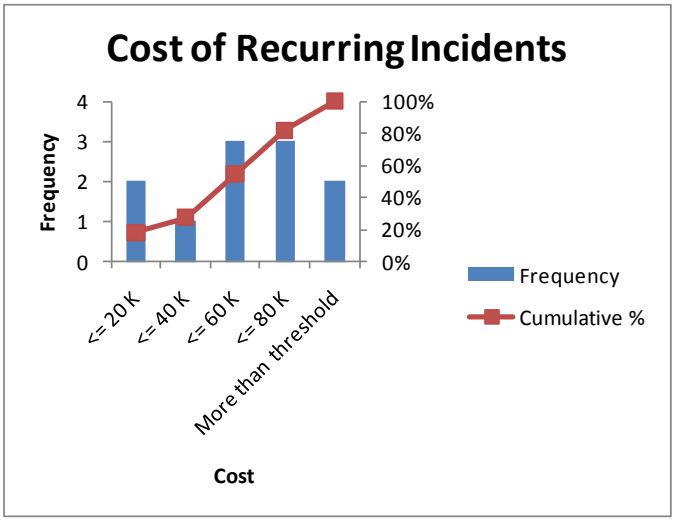
Measure Name/ID	Unique name or identifier for the measure. For example: *Number of Resilience Requirements*
Goal	Statement of resilience goal. Goal should be connected to overall organizational strategic goals and critical success factors, organizational resilience goals, service resilience goals, and/or asset resilience goals.
Question(s)	What question(s) is the measure intending to answer? For example: *How many incidents occurred last quarter?* The question should relate to the Goal.
Visual Display	Graphical depiction of the measure. For example: trend over time, percentages, cumulative results, Pareto analysis, frequency diagrams, etc.
Data Input(s) **Data Elements** **Data Type**	Measure Name/ID and type (base or derived) of all input data elements used for this measure.

Data Collection **How** **When/How Often** **By Whom**	How the data will be collected (process), when and how often the data will be collected (event driven, periodic), and who will collect the data (people, tool). Refer to forms or standards if needed.
Data Reporting **By/To Whom** **When/How Often**	Identify the role that is responsible for reporting the measure. Identify for whom (role) the report is intended. This may be an individual role or an organizational unit.
Data Storage **Where** **How** **Access Control**	Identify where the data is to be stored. Identify the storage media, procedures, and tools for configuration control. Specify how access to this data is controlled.
Stakeholders **Information Owner(s)** **Information Collector(s)** **Information Customer(s)**	Who will use this measure? How? What are the roles? For now, refer back to PA for specific roles in that PA. Asset owner, service owner, line of business manager, someone who heads up business continuity, steering group responsible for operational resilience (ORPG - like an SEPG[18]). Consider stakeholders external to the organization.
Algorithm or Formula	Specify the algorithm or formula required to combine data elements to create input values for the measure. It may be very simple, such as input1/input2 or it may be much more complex. The relationship between the algorithm and the visual display should be explained as well.
Interpretation or Expected Value(s)	Describe what different values of the measure mean. Make it clear how the measure answers the Question(s) above. Provide any important cautions about how the measure could be misinterpreted and actions to take to avoid misinterpretation. Provide guidance on how to interpret the measure and also what not to do with the measure. If the measure has a target value or range for success (meeting the goal), include this here.

Table 11 depicts one example of a completed template for a measure of interest. The measure presents information to aid in determining the impact of recurring incidents with known solutions. Refer to Section 4.2 for further details about deriving measures in this problem space along with a few additional examples.

[18] A Software Engineering Process Group has a key role in the implementation of the software development processes defined in CMMI-DEV. The SEPG is typically responsible for identifying and implementing process-based improvements. In CERT-RMM, we suggest an equivalent group (the Operational Resilience Process Group (ORPG)) to perform a similar function.

Table 11: Sample Template for Measuring the Impact of Recurring Incidents with Known Solutions

Measure Name/ID	Cost of recurring incidents	
Goal	O6: In the face of realized risk, the ORM program ensures the continuity of essential operations of high-value services and associated assets.	
Question(s)	How many incidents with impact greater than X and with known solutions have recurred during the last reporting period?	
Visual display		
Data Input(s) **Data Elements** **Data Type**	Start date of last reporting period	Base measure of type "schedule"
	End date of last reporting period	Base measure of type "schedule"
	Number of recurring incidents during the last reporting period	Base measure of type "count"
	Impact of each recurring incident (cost or effort)	Base measure of type "cost"
	Impact threshold	Base measure of type "cost"
Data Collection **How** **When/How Often** **By Whom**	• Information about an incident is collected throughout the incident management process, on an event-driven basis, by the organization's service desks. • Information is reviewed either when the incident is closed (IMC:SG4.SP4 Close Incidents) or when the post-incident review is performed (IMC:SG5.SP1 Perform Post-Incident Review during post-incidence review). • Impact threshold is established by the Chief Information Security Officer (CISO) and is informed by risk management.	
Data Reporting **By/To Whom** **When/How Often**	• Data is reported to CISO by Computer Security Incident Response Team (CSIRT). • Data is reported once per reporting period.	
Data Storage **Where** **How** **Access Control**	• Data is stored in incident knowledgebase. • All incident report records contain cost information. • All incident report records contain recurrence information. • Everyone has read access to the incident report database. • Only CSIRT has write access to the incident report database.	
Stakeholders **Information Owner(s)** **Information Customer(s)**	• The CISO is the owner of the incident knowledgebase. • The CISO establishes the impact threshold. • The CISO and senior management are the customers for this information. • The Incident Owner is responsible for maintaining and presenting all information related to an incident. • The staff responsible for managing incidents validates the measures and may be called upon to act on the results. *(IMC:SG1.SP2 Assign Staff to the Incident Management Plan)*	

Algorithm or Formula

Each incident record in the incident knowledgebase must contain the following information:

Variable	Type
Date of Occurrence	Date
Cost	Effort Hours or Currency
Occurred before	Boolean

Other information needed:

Variable	Type
Start of Reporting Period	Date
End of Reporting Period	Date
Impact threshold	Effort Hours or Currency

Algorithm steps to create frequency histogram

1. Create cost bins for the frequency histogram. All costs greater than the established impact threshold should be counted in the last bin.
2. For all incidents in the incident knowledgebase where ("Start of Report Period" < "Date of Occurrence" <= "End of Reporting Period") ***and*** ("Occurred before" is True)
    a. Get "cost" of incident.
    b. Increment frequency of the bin the cost falls into.
    c. Increment cumulative percentage of items in bins.

Example input data:

Incident Number	*Incident Cost (in thousands of dollars)*	*Incident Occurred Before?*		*Impact Threshold (in thousands of dollars)*
1	87	Yes		80
2	23	No		
3	27	Yes		
4	45	No		
5	20	No		
6	45	Yes		
7	62	Yes		
8	7	No		
9	3	Yes		
10	52	Yes		
11	20	Yes		
12	29	No		
13	43	Yes		
14	44	No		
15	92	Yes		
16	66	No		
17	74	Yes		
18	61	Yes		

	Example output data: Plot Frequency and Cumulative % on the Y-axis, and Cost bins on the X-axis.
Interpretation or Expected Value(s)	All recurring incidents that cost more than the established organization threshold should be referred to the *(business process that handles this).* Any incident in the bin labeled ***above threshold*** is cause for concern. The heights of the bins represent the number of recurring incidents whose costs fall in that bin. Therefore, the higher the height of the last bin, the greater the concern.

Cost	*Frequency*	*Cumulative %*
<= 20 K	2	18.18%
<= 40 K	1	27.27%
<= 60 K	3	54.55%
<= 80 K	3	81.82%
More than threshold	2	100.00%

The next two sections describe the relationship of the measurement template to two CERT-RMM process areas that have measurement as their principle focus: Measurement and Analysis (MA) and Monitoring (MON). The concepts and approach described in this report can largely be addressed by implementing these two process areas. In addition, the measurement template provides a detailed specification that can be used to meet several of the goals and practices in MA and MON.

3.3.1 Relationship to the Measurement and Analysis Process Area

The Measurement and Analysis (MA) process area "develops and sustains a measurement capability that is used to support management information needs for managing the operational resiliency management process." [Caralli 2010a]

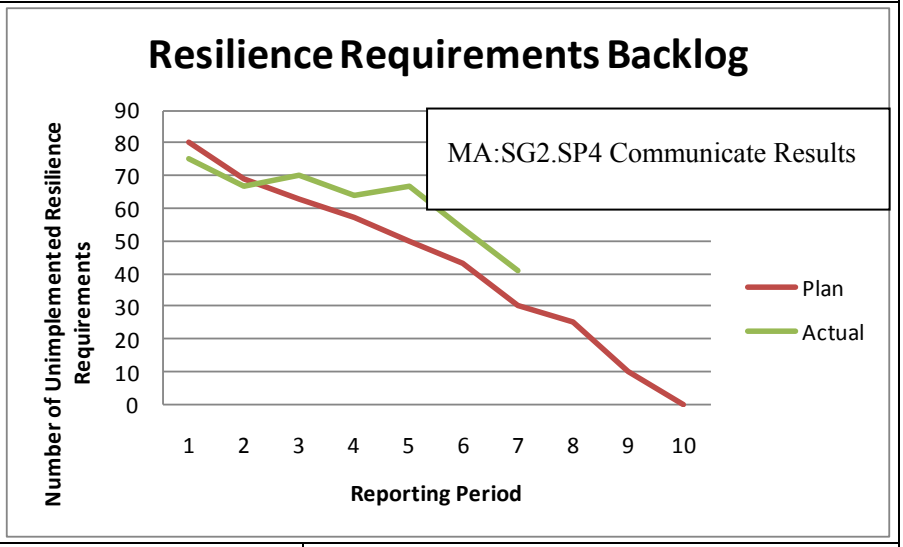
Organizations implementing the MA PA may find that the measurement template provides tactical support for specifying and documenting data collection, storage, analysis, and reporting procedures. Since the MA PA is linked to every other CERT-RMM PA via an institutionalization practice (Generic Goal 2 Generic Practice 8), the template also supports this generic practice for each PA.

Table 12 shows the specific goals (SGs) and specific practices (SPs) for the MA PA. Table 13 shows how MA specific goals and specific practices map to different elements in the measurement template.

Table 12: Measurement and Analysis PA Specific Goals and Specific Practices

Goals	**Practices**
MA:SG1 Align Measurement and Analysis Activities	MA:SG1.SP1 Establish Measurement Objectives
	MA:SG1.SP2 Specify Measures
	MA:SG1.SP3 Specify Data Collection and Storage Procedures
	MA:SG1.SP4 Specify Analysis Procedures
MA:SG2 Provide Measurement Results	MA:SG2.SP1 Collect Measurement Data
	MA:SG2.SP2 Analyze Measurement Data
	MA:SG2.SP3 Store Data and Results
	MA:SG2.SP4 Communicate Results

Table 13: Mapping Measurement and Analysis PA to Measurement Template

Measure Name/ID	
Goal	MA:SG1.SP1 Establish Measurement Objectives
Question(s)	
Visual display	
Data Input(s) **Data Elements** **Data Type**	MA:SG1.SP2 Specify Measures
Data Collection **How** **When/How Often** **By Whom**	MA:SG1.SP3 Specify Data Collection and Storage Procedures MA:SG2.SP1 Collect Measurement Data
Data Reporting **By/To Whom** **When/How Often**	MA:SG2.SP4 Communicate Results
Data Storage **Where** **How** **Access Control**	MA:SG1.SP3 Specify Data Collection and Storage Procedures MA:SG2.SP3 Store Data and Results
Stakeholders **Information Owner(s)** **Information Collector(s)** **Information Customer(s)**	
Algorithm or Formula	MA:SG1.SP4 Specify Analysis Procedures MA:SG2.SP2 Analyze Measurement Data
Interpretation or Expected Value(s)	

3.3.2 Relationship to the Monitoring Process Area

The second process area in CERT-RMM to focus on measurement is the Monitoring (MON) PA. "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 is an enterprise-wide activity that the organization uses to 'take the pulse' of its day-to-day operations and, in particular, its operational resilience management processes." [Caralli 2010a]

The MON PA focuses on the collection and distribution of information, much of which is collected using automated tools. There is very little analysis done in this PA. Within the IT operations community, this is a well known and implemented practice concerned with monitoring the status and health of the network infrastructure and all of the devices connected to it. This includes security monitoring (firewalls, intrusion detection, suspicious or unexpected behavior) and monitoring for disruptive events that fall within the scope of business continuity.

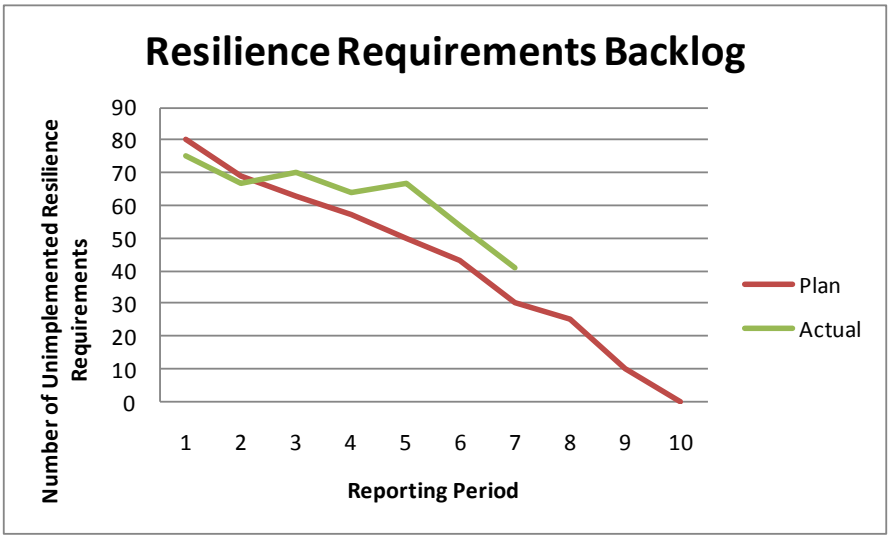
Organizations implementing the MON PA may find that the measurement template provides tactical support for specifying and documenting data collection, storage, and reporting procedures. MON is linked to every other CERT-RMM PA via an institutionalization practice (Generic Goal 2 Generic Practice 8). Thus, the template also supports this generic practice for each PA.

Table 14 shows the specific goals (SGs) and specific practices (SPs) for the Monitoring PA. Table 15 shows how some of these specific goals and specific practices map to different elements in the measurement template.

Table 14: Monitoring Process Area Specific Goals and Specific Practices

Goals	Practices
MON:SG1 Establish and Maintain a Monitoring Program	MON:SG1.SP1 Establish Monitoring Program
	MON:SG1.SP2 Identify Stakeholders
	MON:SG1.SP3 Establish Monitoring Requirements
	MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements
MON:SG2 Perform Monitoring	MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure
	MON:SG2.SP2 Establish Collection Standards and Guidelines
	MON:SG2.SP3 Collect and Record Information
	MON:SG2.SP4 Distribute Information

Table 15: Mapping the Monitoring PA to the Measurement Template

Measure Name/ID		
Goal		
Question(s)		
Visual display		
Data Input(s)		

Data Elements **Data Type**		
Data Collection **How** **When/How Often** **By Whom**	MON:SG2.SP2 Establish Collection Standards and Guidelines MON:SG2.SP3 Collect and Record Information	
Data Reporting **By/To Whom** **When/How Often**	MON:SG2.SP4 Distribute Information	
Data Storage **Where** **How** **Access Control**	MON:SG2.SP3 Collect and Record Information	
Stakeholders **Information Owner(s)** **Information Collector(s)** **Information Customer(s)**	MON:SG1.SP2 Identify Stakeholders	
Algorithm or Formula		
Interpretation or Expected Value(s)		

To clarify the relationships between the Measurement and Analysis (MA) process area, the Monitoring (MON) process area, and Generic Goal 2: Generic Practice 8 (GG2.GP8) Monitor and Control the Process that appears in every process area, we offer the following:

- The MON PA describes the collection and distribution of data, much of which is performed using automated tools. Monitoring is a well known and implemented practice in the IT operations community, for monitoring the status and health of the network infrastructure and all of the devices connected to it. This includes security monitoring (firewalls, intrusion detection, suspicious or unexpected behavior) and monitoring for disruptive events that fall within the scope of business continuity. There is very little analysis done in the MON PA.
- The MA PA defines a measurement program that includes defining, analyzing, and reporting measures that are meaningful to the organization. The content of this report is one expression of a framework that fits within the scope of the MA PA. Data from MON is one of the sources for MA. MA:SG2.SP1 Collect Measurement Data mentions receiving input from MON. It also describes higher level data collection and definition (such as base and derived measures) that is beyond the scope of MON.
- It may be helpful to think of the MON PA as raw data collection and to think of the MA PA as receiving input from MON (and other sources), and then defining, analyzing, and reporting meaningful measures.
- Some of the confusion between the MON PA and GG2.GP8 is the GG2.GP8 title – Monitor and Control the Process. This title was retained for parity with CMMI-DEV. If this practice was accurately titled, it would read "Measure the Process." GG2.GP8 is the instantiation of the MA process area at capability level 2 for each PA.

We refer the reader to CERT-RMM for additional details.

4 Example Resilience Measurement Scenarios

As described in *CERT Resilience Management Model*, operational resilience management encompasses many disciplines and practices [Caralli 2010a]. Once an organization understands the process area relationships in the CERT-RMM model—and is able to connect these with its own operational resilience management processes—it will be able to easily identify the most relevant resilience processes.

There are two types of process area relationships within CERT-RMM that are useful to understand when selecting objectives, questions, and resilience processes for measurement and analysis. The *model view* aids in understanding process relationships from a CERT-RMM model architecture perspective. The way that process areas are grouped provides perspective on the area of operational resilience management that those process areas are intended to support. The model view organizes the 26 CERT-RMM process areas into four categories: Enterprise Management, Engineering, Operations, and Process Management.

The *objective view* helps explain the model through process area relationships that support a particular goal and objective. For example, if the objective is to improve the management of vulnerabilities to high-value information assets, the objective view links together the process areas that satisfy this objective. Because CERT-RMM allows an organization to develop an approach to improvement that addresses specific objectives, understanding the process areas that contribute to meeting the objective is important in selecting meaningful areas for process improvement, and to measure their implementation, effectiveness, and process performance (refer to Section 3.1.3).

Understanding the key relationships that exist among resilience processes helps organizations focus their improvement actions and provides essential context for identifying meaningful measures that help determine if they are meeting their operational resilience objectives. In this section, we select three example views (one model view, two objective views) of related process areas and present one measurement example in the context of each view. As the model continues to be used and adopted, additional objectives and process area relationships will be developed and described along with measures that are providing value to CERT-RMM users.

4.1 Relationships that Drive the Management of Risk: An Enterprise Management Model View

At the enterprise level, the organization establishes and conducts many activities that set the tone for operational resilience, such as governance, risk management, compliance, financial responsibility, and service continuity.

For measurement purposes, it is important to understand that these processes represent organization-wide competencies that affect the operational resilience of organizational units. As a result, many of them map directly to the ORM program objectives defined in Section 2. The implementation of such processes should be performed at the enterprise level for optimal effectiveness. That said, they are often implemented at the level of an organizational unit in the absence of the companion enterprise-level capability. As an example, those performing measurement and analysis need to keep in mind that practices in the Risk Management process area may be performed by an

organizational unit but their effectiveness may be limited by the overall risk management capability of the organization[19].

Figure 4 depicts the relationships that drive the management of risk at the enterprise level, as one aspect of the Enterprise Management category. We refer to this figure as the risk "ecosystem," the collection of process areas, relationships, goals, and practices that contribute to the effective management of risk.[20]

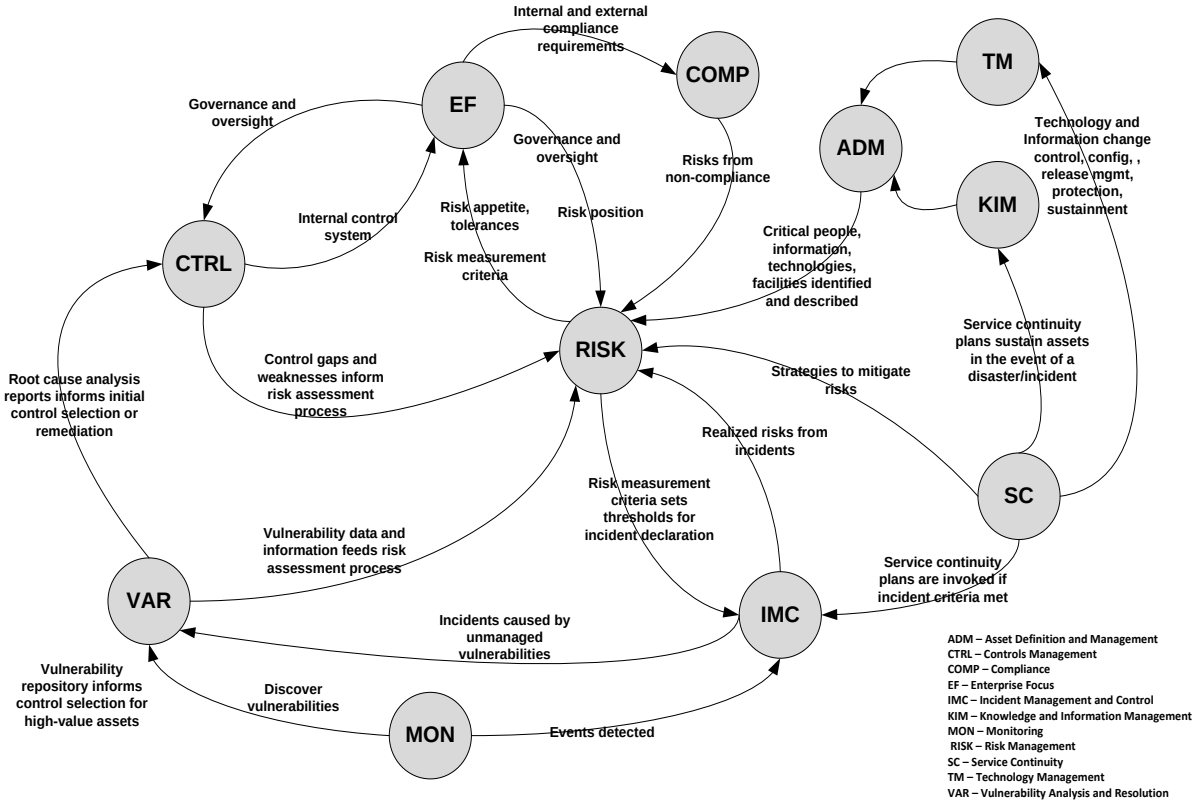


Figure 4: Relationships that Drive the Management of Risk: The Risk Ecosystem

4.1.1 Deriving an Example Measure for Managing Risk

Managing risk involves identifying, analyzing, and mitigating risk within acceptable risk thresholds.[21] Using the relationships depicted in Figure 4, we select a general topic of interest around identifying risk as the first aspect of effective risk management. Risks can arise from all of the process areas shown in Figure 4, so when identifying risks for the purpose of measurement, all

---

19 A more detailed description of the Enterprise Management category and the process areas that compose it can be found in [Caralli 2010a].

20 The concept and use of ecosystems as expressions of model and objective views is more fully described in [Caralli 2010a].

21 Refer to the RISK PA for more information.

sources of risk need to be considered (refer to the sample measure and template described in Step 5).

We use the following process to aid in determining meaningful measures to identify risk. This is a variation of the GQ(I)M method described in Section 3.2 and illustrated in Section 2.3

1. Select an ORM program objective for which information is needed including measurement information.
2. Formulate the question(s) about what you want to know or learn about the ORM program objective.
3. Identify the information that is needed to answer the question(s).
4. Identify key measures and related indicators that provide the needed information.
5. Develop definitions of these measures and fill out a measurement template (refer to Section 3.3). The data presented in each of the example templates that appear in this section is for illustration only (i.e., the templates do not reflect actual data).
6. Based on this analysis, identify updates to the model process area example measures described in the relevant process area's Generic Goal 2: Generic Practice 8 Monitor and Control the Process.

Step 1: Select objective

The ORM program objective to which the topic of identifying risk most closely relates is *Objective O5: The ORM program manages (identifies, analyzes, mitigates) operational risks to high-value assets that could adversely affect the operation and delivery of high-value services.*

Step 2: Formulate question

One of the key questions for identifying risk is: How do I determine if/how confident am I that the risk ecosystem (Figure 4) has identified the highest priority risks (those that I need to pay most attention to; invest most resources to mitigate)?

A useful companion question (which is not analyzed in this section) replaces "identified" above with "mitigated:" How do I determine confidence that the risk ecosystem has *mitigated* the highest priority risks (those that need the most attention and the most resources to mitigate)?

Step 3: Identify information

The following information includes that which is needed to address the "identify risk" question:[22]

- a confidence factor that all risks that need to be identified have been identified
- categorized risks (by risk source, by asset, by service)
- risk parameters and measurement criteria by risk category
- risks categorized and prioritized by parameters

[22] Refer to the RISK PA for definitions and use of terms.

- risks that exceed parameters with a disposition of "mitigate and control"

Step 4: Identify key measures and indicators

A few of the more interesting or informative key measures that provide some of the needed information include:

- confidence factor
- number/percentage of identified risks that exceed parameters
- percentage of risks (by asset, by service) that
  - exceed parameters
  - have a disposition of mitigate or control
  - have (do not have) defined, implemented mitigation plans

One of the more informative measures for addressing the companion question in Step 2 is the effectiveness of mitigation plans in moving risk to be within/below parameters.

Step 5: Complete measurement template

Confidence factor as a measure is one of the more challenging measures so we opted to select this one to see if we could actually derive a meaningful measure based on the concepts and template presented in Section 3. We first define a measure for expressing confidence that risks from all sources have been identified. Armed with this information, we can then define a measure around confidence in having identified the highest priority risks. This is a next step to be completed.

One way to determine confidence factor that risks from all sources have been identified is to consider the following series of questions:

1. Do all organizations in the enterprise have defined risk parameters? (RISK PA)

2. Have all lines of business in the organization derived risk parameters based on the organization's risk parameters? (RISK PA)

3. Have risks for all assets in the asset database been defined considering all sources of operational risk (failed internal processes, inadvertent or deliberate actions of people, problems with systems and technology, external events)? (ADM, KIM, TM, CTRL, COMP, IMC, VAR, SC PAs)

4. Have risks for all services in the service inventory been defined considering all sources of operational risk (failed internal processes, inadvertent or deliberate actions of people, problems with systems and technology, external events)? (EF, CTRL, COMP, IMC, VAR, SC PAs)

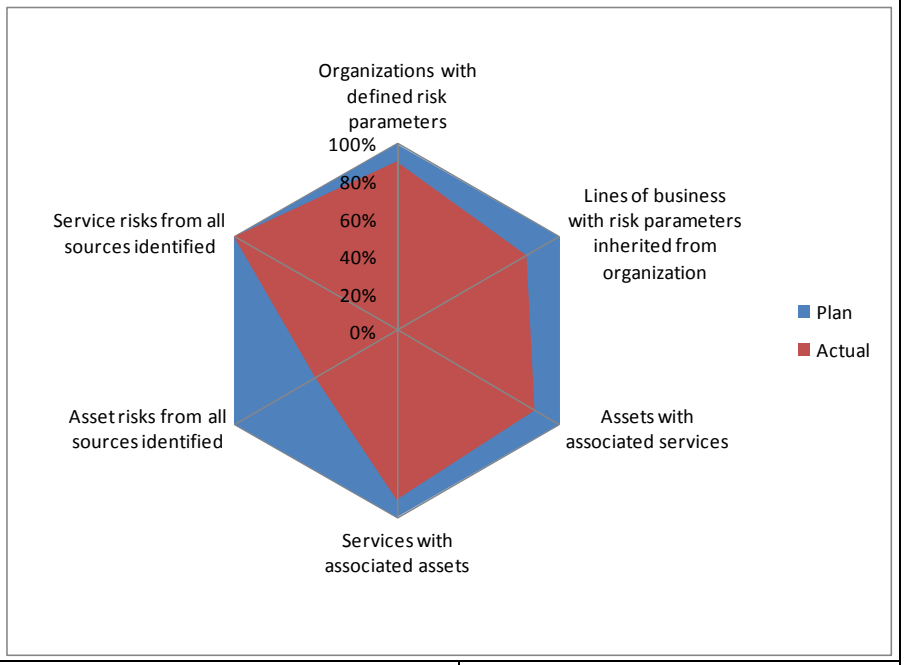
5. Is each asset in the asset database used by at least one service in the service repository? Each asset in the asset database must be used by one or more services. We need to check this 1:m (one-to-many) relationship between an asset and services to make sure that asset risks are identified in the context of the service using the asset. (ADM, EF PAs)

6. Does each service in the service repository use assets from the asset database? Each service can use one or more high-value assets. We need to make sure that each asset used by

a service (1:m relationship between service and asset) is in the asset database to make sure that asset risks have been identified. (ADM, EF PAs)

A confidence factor could be derived by multiplying the percentages of "yes" answers to each of the questions above. Table 16 provides one candidate confidence factor measure using the resilience measurement template.

Table 16: Confidence Factor Measurement Template

Measure Name/ID	Confidence in risk identification	
Goal	O5: The ORM program manages (identifies, analyzes, mitigates) operational risks to high-value assets that could adversely affect the operation and delivery of high-value services.	
Question(s)	Have risks from all sources been identified?	
Visual display		
Data Input(s) **Data Elements** **Data Type**	List of organizational units in enterprise	No data type: this is an attribute of the enterprise.
	List of lines of business per organization	No data type: this is an attribute of the organization.
	List of high-value assets	N/A
	List of high-value services	N/A
	List of risk sources	N/A
	Start date of last reporting period	Base measure of type "schedule"
	End date of last reporting period	Base measure of type "schedule"
Data Collection **How** **When/How Often** **By Whom**	• List of organizations is collected from the enterprise organization chart. • List of lines of business per organization is collected from each organization's organization chart. List of high-value services is collected from the service repository (EF:SG1.SP3 Establish Organizational Services). • List of high-value assets is collected from the asset database (ADM:SG1.SP1 Inventory Assets). • List of risk sources is predefined as failed internal processes, inadvertent or deliberate actions of people, problems with systems and technology, external events. Data is collected by the operational resilience process group (ORPG), once per reporting period.	

Data Reporting **By/To Whom** **When/How Often**	Data is reported by the ORPG to the CISO once per reporting period. The confidence factor report is generated by a report generation tool.
Data Storage **Where** **How** **Access Control**	The confidence factor reports are archived on the CISO SharePoint web site by the ORPG. Only the ORPG has write access to the site. The CISO staff has read access.
Stakeholders **Information Owner(s)** **Information Collector(s)** **Information Customer(s)**	• The information in the asset database is owned by the CISO. • The information in the service repository is owned by the CISO. • Organizational charts and lines of business charts are owned by HR. • The CISO is the primary customer for this report.
Algorithm or Formula	1. Determine the percent of organizations with defined risk parameters (Percent_Orgs). 2. For each organization, identify lines of business. Determine the percent of lines of business with defined risk parameters inherited from parent organization (Percent_LOBs). 3. From the service repository, determine the percentage of services where risks have been identified from all four sources (Percent_Services). 4. From the asset database, determine the percentage of assets where risks have been identified from all four sources (Percent_Assets). 5. From the asset database and service repository, determine the percent of assets used by at least one service (Asset_Usage_By_Services), and the percent of services where all associated assets are in the asset database (Service_Usage_Of_Assets). Confidence = Percent_Orgs * Percent_LOBs * Percent_Services * Percent_Assets * Asset_Usage_By_Services * Service_Usage_Of_Assets
Interpretation or Expected Value(s)	The goal is for the plan and actual axis on the radar plot to be as close as possible, to indicate the actual confidence level is close to the planned confidence level. Overall confidence factor can be determined by multiplying the actual percentage of each axis. A confidence factor of 100% means that all organizations in the enterprise have established risk parameters, that all lines of business in each organization have derived their own risk parameters from their parent organization, that risks from all sources have been identified for all services in the service repository, that risks from all sources have been identified for all assets in the asset database, that all services use assets defined in asset database, and that all assets in the asset database are used by at least one service. If there are other factors that should contribute to this measure, they can be easily added.

Step 6: Identify updates

We examined and analyzed the RISK:GG2.GP8 example measures that appear in CERT-RMM v1.0 to see if any of these might provide useful input to the list of candidate measures identified in Step 4. In the process, we categorized each of the RISK:GG2.GP8 measures in a number of dimensions (refer to Section 3) and identified a number of updates to these. Table 17 presents the results of this analysis. These changes will be considered in the next update to the model.

Table 17: Revised Measures for RISK Generic Goal 2: Generic Practice 8 Monitor and Control the Process

ID[23]	Measure	Type of Information	Measure Type	Base vs. Derived
M1	percentage of identified assets and services for which some form of risk assessment has been performed and documented as required by policy	source[24] of risk (identify)	impl	derived

[23] The ID value is assigned based on the order in which the measure appears in CERT-RMM v1.0 RISK:GG2.GP8. Measures have been reordered here by the type of information.

[24] We likely need to add some new metrics around other sources of risk or make this measure more generic.

M2	percentage of high-value assets and services for which the impact or cost of compromise of a realized risk *(refer to RISK:SG2.SP2)* has/has not been quantified	risk valuation (identify)	impl	derived
M3	percentage of identified risks that do/do not have a defined risk disposition	risk disposition (identify)	impl	derived
M7	percentage of previously identified risks that have converted from any other risk disposition to a risk disposition of "mitigate or control"	risk disposition (identify)	impl	derived
M12	percentage of identified risks that have been characterized as "high" impact according to the organization's risk parameters and measurement criteria	risk disposition (identify)	impl	derived
M4	percentage of identified risks with a disposition of "mitigate or control" that have a defined mitigation plan against which status is reported in accordance with policy	risk mitigation	impl	derived
M8	percentage of high-value assets for which a mitigation plan has been implemented to mitigate risks as necessary and to maintain these risks within acceptable risk parameters	risk mitigation	impl	derived
M9	percentage of high-value services for which a mitigation plan has been implemented to mitigate risks as necessary and to maintain these risks within acceptable risk parameters	risk mitigation	impl	derived
M5	percentage of identified risks that have/have not been tracked to closure	risk status	impl	derived
M6	change in volume of identified risks that exceed risk parameters and measurement criteria	risk status	impl	derived
M11	percentage of realized risks that have exceeded established risk parameters and measurement criteria (duplicates M10)	risk status	impl	derived
M10	percentage of security incidents that caused damage, compromise, or loss to identified assets or services beyond established risk parameters and measurement criteria May want to restate as the percentage of **realized** risks by category [that caused damage, compromise, or loss to identified assets or services beyond; that exceeded] established risk parameters and measurement criteria. There are many additional sources of risk than security incidents; or may want to specifically call out those that are of greatest interest (incidents, control gaps, non-compliance, vulnerabilities, disruptions on continuity, etc.) (duplicates M11)	risk status	impl	derived
M13	level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved	global measure	impl	base of scale ordinal/ratio, type count
M14	number of process activities that are on track per plan	global measure	impl	base of scale ratio, type count
M15	rate of change of resource needs to support the process	global measure	impl	derived
M16	rate of change of costs to support the process	global measure	impl	derived

	New measures			
	confidence factor (likelihood; high, medium, low?) that all risks that need to be identified have been identified	source of risk (identify)	effectiveness	derived
	percentage of identified risks that exceed established risk parameters and measurement criteria by risk category (some overlap with M12)	risk valuation risk disposition (identify)	impl	derived
	number and percentage of risks with a "mitigate or control" disposition without mitigation plans	risk mitigation	impl	base of scale ratio, type count; derived
	number and percentage of risks with a "mitigate or control" disposition with mitigations that are not yet started and in progress (vs. completely implemented)	risk mitigation	impl	base of scale ratio, type count; derived
	extent to which current risks with a "mitigate or control" disposition are effectively mitigated by their mitigation plans	risk mitigation	effectiveness	base of scale ordinal, type count
	elapsed time since risks with the following dispositions were last reviewed and disposition confirmed: avoid, accept, monitor, research or defer, transfer	risk status	impl	base of scale ratio, type schedule
	(addition to M14) number of process activities approved but not implemented (due to, for example, schedule and resource constraints)	global measure	impl	base of scale ratio, type count

The identification of this range and type of updates is another useful outcome from the measurement and analysis research project.

In the next section, we apply this same step-by-step process to an aspect of threat and incident management.

4.2 Relationships that Drive Threat and Incident Management: An Operations Model View

The Operations process areas[25] represent the core activities for managing the operational resilience of assets and services in the operations life-cycle phase. These process areas are focused on sustaining an adequate level of operational resilience as prescribed by the organization's strategic drivers, critical success factors, and risk appetite. These process areas represent core security, business continuity, and IT operations and service delivery management activities and focus specifically on the resilience of people, information, technology, and facilities assets.

Threat, Vulnerability, and Incident Management address the organization's continuous cycle of identifying and managing threats, vulnerabilities, and incidents to minimize organizational disruption. Figure 5 depicts the relationships that drive the management of incidents at the enterprise level, as one aspect of the Operations category. We refer to this figure as the incident management ecosystem, the collection of process areas, relationships, goals, and practices that contribute to the effective management of threats, vulnerabilities, and incidents.

[25] Refer to *CERT Resilience Management Model* for a more detailed description of this category [Caralli 2010a].

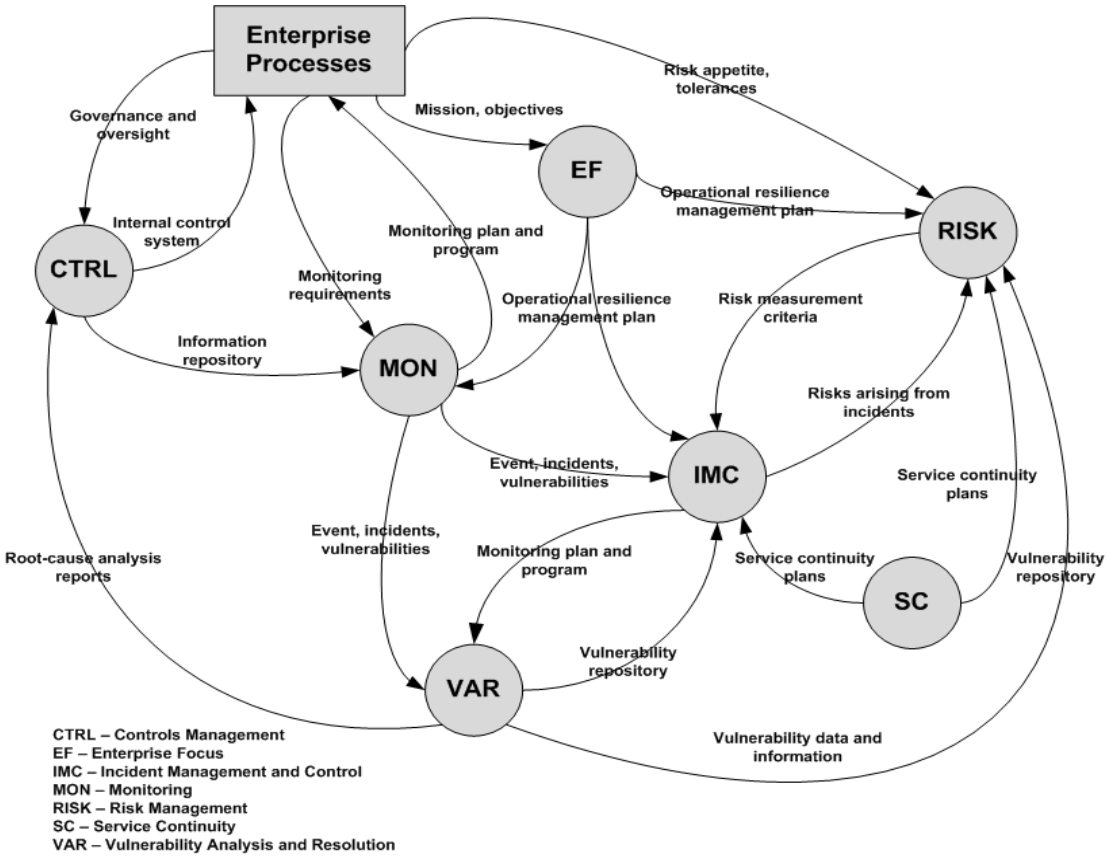


Figure 5: Relationships that Drive Threat and Incident Management: The Incident Management Eco-system

4.2.1 Deriving an Example Measure for Managing Incidents

Managing incidents involves identifying and analyzing events, determining which of these are incidents, and formulating and enacting an appropriate organizational response.[26] Using the relationships depicted in Figure 5, we select a general topic of interest around identifying incidents with known root causes (likely with known solutions) as a key aspect of effective incident management. Continuing to experience incidents that are caused by known problems (including inadequate or missing controls) with known solutions is, at best, a distraction and, at worst, consumes time, resources, and attention that are better applied to productive work. It would be worthwhile to gain insight into which root causes lead to the most expensive incidents, and which root causes lead to the highest number of incidents. Armed with this information, organizations can then focus on developing solutions for the root causes with the highest payoffs.

We use the same process for identifying incidents with known root causes as described in Section 4.1.

Step 1: Select objective

The ORM program objective to which the topic of identifying incidents with known root causes most closely relates is *Objective O6: In the face of realized risk, the ORM program ensures the*

[26] Refer to the IMC PA.

continuity of essential operations of high-value services and their associated assets. An incident is a category of realized risk.

Step 2: Formulate question

Some of the key questions for identifying incidents with known root causes are: Have I seen this incident (or this set of events leading up to the declaration of an incident) before, did I resolve it in the past and if so how, and how many incidents with impact (for example, cost) greater than "x" resulted from a known root cause with a known solution? ("x" is an expression that takes into account risk appetite, tolerance, thresholds, impact, and likelihood (measurement criteria) as defined in the RISK process area.) A reasonable response to incidents less than impact "x" is to accept and manage them as a normal cost of doing business. Measures of interest include frequency of occurrence (how often do incidents with known root causes occur) and the root causes of the costliest incidents over a designated reporting period.

A useful companion question (which is not analyzed in this section) is: Is the criteria for declaring an incident (based on all related events) sufficiently robust and defined to ensure that incidents with potential impact greater than "x" are detected?

Step 3: Identify information needs

For the purpose of this scenario, we select the question "what are the root causes of the costliest incidents." The information that is needed to address this question includes[27]

- event reports that have been categorized, correlated, prioritized, and have an assigned disposition of "declared as an incident." This typically occurs as part of a defined triage process. Knowing the collection of events leading to an incident can be used to inform root cause analysis.
  - incident management knowledge base (or equivalent) that associates events with potential incidents
- open event reports
- incident analysis reports for open and closed incidents including root-cause analysis, incident cost, and other impact-related information
  - incident management knowledge base (or equivalent) that reflects this information and keeps it up to date
- reports from incident analysis tools and techniques
- risk measurement criteria[28]

Step 4: Identify key measures and indicators

A few of the more interesting or informative key measures that provide some of the needed information include:

- average time between event detection and incident declaration

---

[27] Refer to the IMC PA for definitions and use of terms.

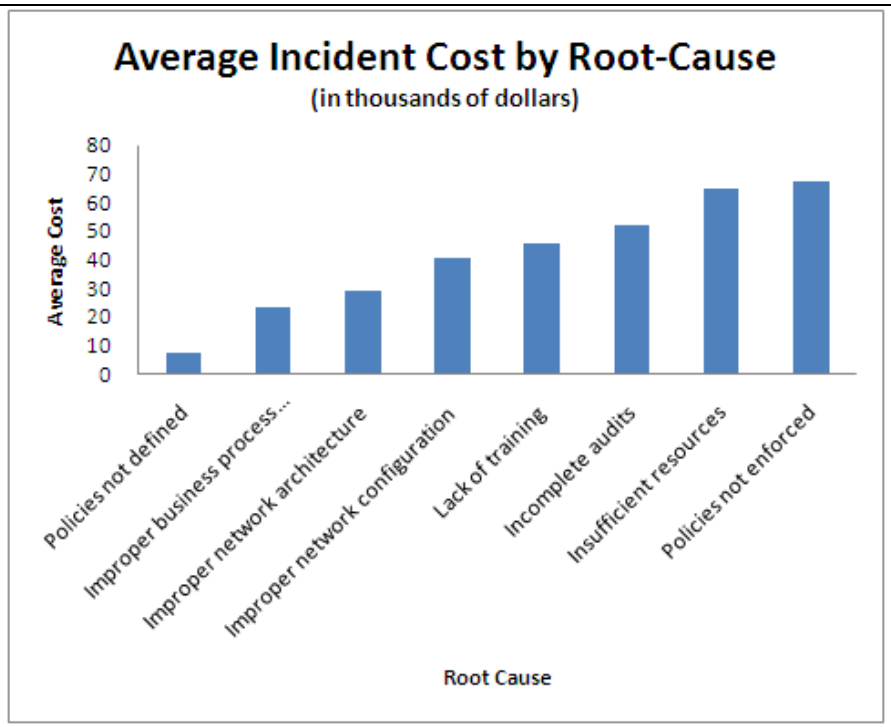
[28] Refer to the RISK PA.

- minimum, mean, and maximum number of events that lead to the declaration of an incident
- percentage of closed incidents with impact greater than x, categorized by root cause (may also be categorized by asset, by service, by incident type)
  - in the last reporting period
  - in the current reporting period
  - comparison of last period percentages with current period percentages by impact, by root cause
- percentage of open/in progress incidents with potential impact greater than x (categorized by potential root cause) in the current reporting period

Step 5: Complete measurement template

Average incident cost by root cause type for the current reporting period provides a strong indicator to help determine where improved processes and practices are required to minimize and perhaps even eliminate root causes with the highest average cost. A count or percentage of incidents with the most frequently occurring root causes is a useful companion measure. Table 18 provides one candidate definition for the average cost measure using the resilience measurement template.

Table 18: Average Incident Cost by Root Cause Measurement Template

Measure Name/ID	Average incident cost by root cause type	
Goal	O6: In the face of realized risk, the ORM program ensures the continuity of essential operations of high-value services and associated assets.	
Question(s)	What were the root-causes of the costliest incidents during the last reporting period?	
Visual display		
Data Input(s) **Data Elements** **Data Type**	Start date of last reporting period	Base measure of type “schedule”
	End date of last reporting period	Base measure of type “schedule”
	Cost of incidents	Base measure of type “cost”
	Root causes of incidents	

<table>
<tr><td>Data Collection
How
When/How Often
By Whom</td><td>• Information about an incident is collected throughout the incident life-cycle, on an event-driven basis, by the organization's service desks.
• Information is reviewed either when the incident is closed (IMC:SG4.SP4 Close Incidents) or when the post-incident review is performed (IMC:SG5.SP1 Perform Post-Incident Review).
• List of root causes of incidents is maintained by the CSIRT, and updated after each post-incident review.</td></tr>
<tr><td>Data Reporting
By/To Whom
When/How Often</td><td>• Data is reported to CISO by CSIRT.
• Data is reported once per reporting period.</td></tr>
<tr><td>Data Storage
Where
How
Access Control</td><td>• Data is stored in the incident knowledgebase.
• Each incident report record contains cost information.
• Each incident report record contains root cause information.
• Everyone has read access to the incident knowledgebase.
• Only CSIRT has write access to the incident knowledgebase.</td></tr>
<tr><td>Stakeholders
Information Owner(s)
Information Customer(s)</td><td>• The CISO is the owner of the incident knowledgebase.
• The CISO and senior management are the customers for this information.
• The incident owner is responsible for maintaining and presenting all information related to an incident.
• The staff responsible for managing incidents validates the measure and may be called upon to act on the results (IMC:SG1.SP2 Assign Staff to the Incident Management Plan).</td></tr>
<tr><td>Algorithm or Formula</td><td>Each incident record in the incident knowledgebase must contain the following information:

<table>
<tr><th>Variable</th><th>Type</th></tr>
<tr><td>Date of Occurrence</td><td>Date</td></tr>
<tr><td>Cost</td><td>Effort Hours or Currency</td></tr>
<tr><td>Root Cause</td><td>Name or label</td></tr>
</table>

Other information needed:
<table>
<tr><th>Variable</th><th>Type</th></tr>
<tr><td>Start of Reporting Period</td><td>Date</td></tr>
<tr><td>End of Reporting Period</td><td>Date</td></tr>
<tr><td>List of root causes</td><td>Names or Labels</td></tr>
</table>

Algorithm steps to create average-cost-by-root-cause bar chart.

For each root cause in the organization's list of root causes
1. Select all incidents in the incident knowledgebase where ("Start of Report Period" < "Date of Occurrence" <= "End of Reporting Period") and ("Root Cause" = selected root clause)
2. Add "Cost" of all incidents selected based on the above criteria, to calculate Total Cost for selected root cause.
3. Divide Total Cost by the count of incidents based on the above criteria, to calculate Average Cost for selected root cause.</td></tr>
</table>

Example input data:

The following table shows the historical root causes for incidents that have occurred in the organization:

List of Root Causes
Policies not defined
Improper business process design
Improper network architecture
Improper network configuration
Lack of training
Incomplete audits
Insufficient resources
Policies not enforced

The following table shows data collected for each incident:

Incident Number	*Incident Cost (in thousands of dollars)*	*Root Cause*
1	87	Insufficient resources
2	23	Improper business process design
3	27	Lack of training
4	45	Lack of training
5	20	Lack of training
6	45	Lack of training
7	62	Policies not enforced
8	7	Policies not defined
9	3	Improper business process design
10	52	Incomplete audits
11	20	Improper network configuration
12	29	Improper network architecture
13	43	Insufficient resources
14	44	Improper business process design
15	92	Lack of training
16	66	Policies not enforced
17	74	Policies not enforced
18	61	Improper network configuration

	Example output data: The following table shows both frequency and average cost of incidents by root cause type. *Root Cause* / *Count of Incidents* / *Total Cost of Incidents(in thousands of dollars)* / *Average Cost by Root Cause (in thousands of dollars)* Policies not defined: 1, 7.00, 7.00 Improper business process design: 3, 70.00, 23.33 Improper network architecture: 1, 29.00, 29.00 Improper network configuration: 2, 81.00, 40.50 Lack of training: 5, 229.00, 45.80 Incomplete audits: 1, 52.00, 52.00 Insufficient resources: 2, 130.00, 65.00 Policies not enforced: 3, 202.00, 67.33 Plot *Root Cause* as labels on X-Axis, with *Average Cost by Root Cause* on the Y axis.
Interpretation or Expected Value(s)	The bar chart shows the average incident cost per root cause for all incidents reported in the last reporting period. The average costs are sorted in ascending order. The organization should focus improvement activities on addressing those root causes that are the costliest, particularly those that exceed established impact thresholds. Note that a Pareto Analysis could be performed on the same data to focus on the most frequent root causes for incidents. Also note that using the 95th percentile instead of the average alone may be more meaningful. Use of averages alone can often be ill-advised and misleading. The use of the 95th percentile allows accounting for a skewed and unbalanced distribution and is far more informative than the mean.

Step 6: Identify updates

We examined and analyzed the IMC:GG2.GP8 example measures that appear in CERT-RMM v1.0, to see if any of these might provide useful input to the list of candidate measures identified in Step 4. In the process, we identified a number of updates to the current set of IMC:GG2.GP8 measures. Table 19 presents the results of this analysis. These changes will be considered in the next update to the model.

Table 19: Revised Measures for IMC Generic Goal 2: Generic Practice 8 Monitor and Control the Process

ID[29]	Measure	Type of Information	Measure Type	Base vs. Derived
M3	percentage of events triaged in a specific period	event triage	impl	derived
M4	number of events and incidents that occur in a specific period	event; incident detection	impl	base of scale ratio, type count
M2	percentage of incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds	incident analysis	impl	derived
M1	percentage of operational time that high-value services and assets were unavailable (as seen by users and customers) due to inci- dents	incident analysis	impl	derived
M10	extent of consequences to the organization due to incidents by incident type (also referred	incident analysis	impl	derived

[29] The ID value is assigned based on the order in which the measure appears in CERT-RMM v1.0 IMC:GG2.GP8. Measures have been reordered here by the type of information.

	to as magnitude)			
M12	percentage of recurrence of specified events or incidents	event; incident tracking, analysis	impl	derived
M13	percentage increase (decrease) in resource needs (training, skill building, additional human resources) to support incident management	event analysis; incident analysis	impl; could also be effectiveness	derived
M5	percentage of incidents that require escalation	incident escalation	impl	derived
M6	percentage of incidents that require involvement of law enforcement	incident escalation	impl	derived
M9	percentage increase (decrease) in the volume of events and incidents in a specific period	event; incident tracking	impl; could also be effectiveness	derived
M7	percentage of events and incidents that have been logged but not closed	event tracking; incident tracking	impl	derived
M8	average time between event detection and related incident declaration, response, and closure	event tracking; incident tracking	impl; could also be effectiveness	derived
M11	percentage increase (decrease) in the elapsed time of the incident life cycle by incident type	incident tracking	impl; could also be effectiveness	derived
M15	number of incidents referred to the risk management process; number of risks where corrective action is still pending (by risk rank)	incident tracking	impl	base of scale ratio, type count
M14	number of post-incident review activities that result in control changes or improvements to the process	incident post review	impl	base of scale ratio, type count
M16	level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved	global measure	impl	base of scale ordinal/ratio, type count
M17	number of process activities that are on track per plan	global measure	impl	base of scale ratio, type count
M18	rate of change of resource needs to support the process	global measure	impl	derived
M19	rate of change of costs to support the process	global measure	impl	derived
	New measures			
	number and percentage of events that are categorized as incidents	incident analysis	impl	base of scale ratio, type count; derived
	increase/decrease in extent of consequences to the organization due to incidents by incident type (also referred to as magnitude)	incident analysis	impl; could also be effectiveness	derived

In the next section, we apply this same step-by-step process to an aspect of information resilience.

4.3 Relationships that Drive Information Resilience: An Objective View for Information Assets

As stated in *CERT Resilience Management Model*, the importance of information as an organizational asset continues to grow [Caralli 2010a]. Organizations are increasingly focusing on intangible assets and the ratio of tangible assets to intangible assets continues to decrease. This supports the assertion that information is one of the most—if not the most—high-value organizational as-

set. It is the raw material used by and created in services. Protecting and sustaining this intellectual and enterprise capital—to ensure that it is available in the form intended for use in services—is an essential area requiring measurement attention to more effectively manage operational resilience.

An information asset can be described as information or data that is of value to the organization, including such diverse information as patient records, intellectual property, vital business records and contracts, and customer information. The unique aspect of information assets is that they can exist in physical form (e.g., paper, CDs, or other media) or electronic form (e.g., files, databases, on personal computers). The process areas involved in protecting information address the importance of information assets in the operational resilience of services, as well as unique attributes specific to information assets such as those described in Table 20.

Table 20: Attributes of Information Assets

Availability	For an information asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed.
Confidentiality	For an information asset, the quality of being accessible only to authorized people, processes, and devices.
Integrity	For an information asset, the quality of being in the condition intended by the owner and so continuing to be useful for the purposes intended by the owner.
Privacy	The assurance that information about an individual is disclosed only to people, processes, and devices authorized by that individual or permitted under privacy laws and regulations.
Sensitivity	A measure of the degree to which an information asset must be protected based on the consequences of its unauthorized access, modification, or disclosure.

Figure 6 shows the process areas that drive the operational resilience of information. Requirements for protecting and sustaining information are established and utilized by processes such as risk management (RISK), controls management (CTRL), and service continuity (SC).

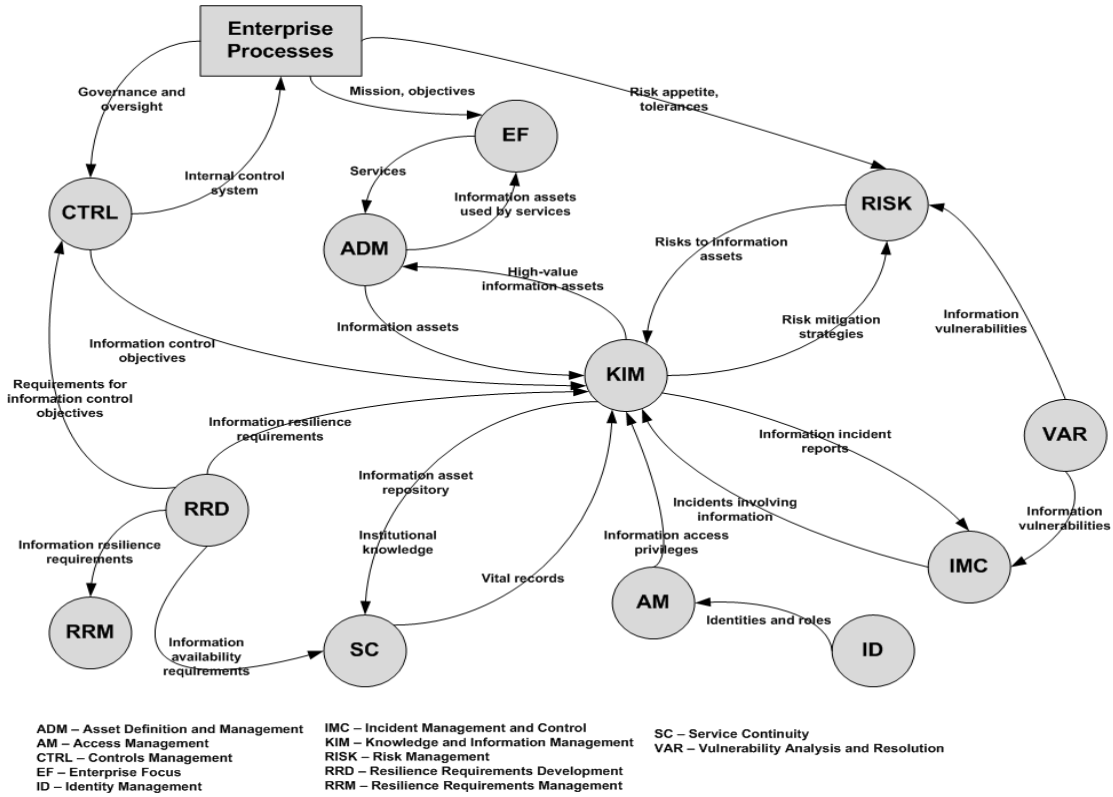


Figure 6: Relationships that Drive Information Resilience: The Information Resilience Ecosystem

4.3.1 Deriving an Example Measure for Protecting Information Assets

Protecting information assets involves ensuring that they are available in support of services and that their information attributes (as shown in Table 20) are preserved throughout their life cycle[30] Using the relationships depicted in Figure 6, we select a general topic of interest around modification of information assets as a key aspect of protecting information assets.

Ensuring that information assets are only modified by authorized staff preserves the integrity of these assets for their intended purposes. A simple way of controlling modification is to control access to these information assets—either electronically (e.g., controlling access to networks, servers, application systems, and databases and files), physically (e.g., by limiting access to file rooms, work areas, and facilities), or both—based on the unique integrity requirements of each information asset. However, because access controls are not infallible, the organization must also log all instances of information asset modification and conduct periodic review of these logs for anomalies.

We use the same process as described in Sections 4.1 and 4.2.

[30] Refer to the Knowledge and Information Management (KIM) PA.

Step 1: Select objective

The ORM program objective to which the topic of information asset modification most closely relates is *Objective O4: Via the internal control system, the ORM program ensures that controls for protecting and sustaining high-value services and their associated assets operate as intended.*

The preservation of information asset integrity is a resilience requirement so Objective O3 may also apply: *The ORM program satisfies high-value asset resilience requirements.*

Step 2: Formulate question

One of the key questions for information asset modification is: how many instances of unauthorized modification of high-value information assets have we experienced?

A useful companion question (which is not analyzed in this section) is: How many cases of unauthorized modification of high-value information assets resulted in the detection of an event and the declaration of an incident with greater than impact "x"?

Step 3: Identify information needs

The information that is needed to address the question above includes[31]

- list of high-value information assets (asset inventory, asset database or equivalent with asset profiles)
- high-value information asset change requests
- information asset modification logs by high-value asset (by asset category, by service)
- reports from log analysis tools
- suspicious or unauthorized access anomalies arising from modification logs, configuration control logs, and audit logs and reports (including the user id of the user making the change)
- changes to high-value information assets without an approved change request (including the user id of the user making the change)

Step 4: Identify key measures and indicators

A few of the more interesting or informative key measures that provide some of the needed information include

- number of physical and logical access controls that have been circumvented, by high-value information asset (by asset category, by service)
- percentage of high-value information assets that have been modified (by asset category, by service)
  - with (without) approved change requests
  - where the modification has been flagged as an anomaly related to suspicious or unauthorized access

[31] Refer to the KIM PA for definitions and use of terms.

Step 5: Complete measurement template

Knowing the instances of high-value information assets that have been modified where the modification has been flagged (by a log analysis tool or other form of analysis) as an access anomaly directly addresses the question. This measure will also aid in identifying control weaknesses, so we opted to select this one. Table 21 provides one candidate definition for this measure using the base measurement template. Since the measure is a simple count of anomalous modifications, a base measurement template is all that is needed.

Table 21: Information Asset Access Anomalies Measurement Template

Measure Name/ID	Number of anomalous modifications to information assets
Measurement Description	Number of high-value information assets that have been modified where the modification has been flagged (by a log analysis tool or other form of analysis) as an access anomaly
Measurement Scale	• Possible set of values: Positive whole numbers only • Scale: Ratio • Units: Number of unauthorized modifications to high-value information assets.
Data Collection **How** **When/How Often** **By Whom**	• High-value information asset access logs are analyzed daily by the access log analysis tools (KIM:SG2.SP2 Establish and Implement Controls, logging controls). • The log analysis tools automatically update the asset database when anomalies are detected (MON:SG2.SP3 Collect and Record Information). • Anomalies are reported daily to the asset custodian. The asset database monitoring program generates a report and e-mails it to the asset custodian (MON:SG2.SP4 Distribute Information). • The data collection method is objective. • The rules for determining when a modification is anomalous are defined by the asset owner, based on the asset's resilience requirements, and are included in the asset profile (ADM:SG3.SP1 Identify Change Criteria).
Data Storage **Where** **How** **Access Control**	• The data is stored in the organization's asset database (ADM ADM:SG1.SP1 Inventory Assets). • Every asset record in the asset database is linked to information about anomalous modification. There is a 1:m (one-to-many) relationship between an asset and information about anomalous modifications. • The asset custodian and asset owner has read access to the asset database. • Only the asset custodian can update the anomalous modification status of the asset (ADM:SG1.SP3 Establish Ownership and Custodianship). • The asset database is backed-up daily.

Step 6: Identify updates

We examined and analyzed the KIM:GG2.GP8 example measures that appear in CERT-RMM v1.0, to see if any of these might provide useful input to the list of candidate measures identified in Step 4. In the process, we identified a number of updates to the current set of KIM:GG2.GP8 measures. Table 22 presents the results of this analysis. These changes will be considered in the next update to the model.

Table 22: Revised Measures for KIM Generic Goal 2: Generic Practice 8 Monitor and Control the Process

ID[32]	Measure	Type of Information	Measure Type	Base vs. Derived
M1	percentage of information assets that have been inventoried	asset inventory	impl	derived
M2	level of discrepancies between actual inventory and stated inventory	asset inventory	impl	ordinal

[32] The ID value is assigned based on the order in which the measure appears in CERT-RMM v1.0 IMC:GG2.GP8. Measures have been reordered here by the type of information.

M3	number of changes made to the information asset inventory during a stated period	asset inventory	impl	base of scale ratio, type count
M4	percentage of information assets that do not have stated owners or custodians	asset profile	impl	derived
M5	percentage of information assets with incomplete descriptions or other incomplete information (particularly the lack of stated resilience requirements)	asset profile	impl	derived
M10	number of physical or logical access controls that have been circumvented; as a result, number of attempted or successful intrusions to technology assets or facility assets where information assets "live"; as a result, number of information assets that have been accessed in an unauthorized manner	access to assets	impl	base of scale ratio, type count
M11	number of information assets for which encryption is required and is yet to be implemented	asset confidentiality	impl	base of scale ratio, type count
M12	frequency and timeliness of information asset backups	asset availability	impl	base of scale ratio, type schedule
M13	frequency of information asset backup restoration testing	asset availability	impl	base of scale ratio, type schedule
M7	percentage of high-value information assets for which the cost of compromise (loss, unauthorized access, disclosure, disruption in access to) has been quantified	asset evaluation	impl	derived
M6	percentage of high-value information assets for which some form of risk assessment has been performed as required by policy	asset evaluation	impl	derived
M16	number of information asset and process risks referred to the risk management process; number of risks where corrective action is still pending (by risk rank)	asset evaluation	impl	base of scale ratio, type count
M14	frequency with which the monitoring logs are validated and placed under configuration control	asset evaluation	impl	base of scale ratio, type schedule
M15	number of policy violations related to confidentiality and privacy of information assets (consider as a qualifier to M17)	asset evaluation	impl	base of scale ratio, type count
M8	level of adherence to external entity service level agreements and agreed maintenance levels for information assets subject to external entity services	asset evaluation	impl	base of scale ordinal, type count
M17	level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved	global measure	impl	base of scale ordinal/ratio, type count
M18	number of process activities that are on track per plan	global measure	impl	base of scale ratio, type count
M19	rate of change of resource needs to support the process	global measure	impl	derived
M20	rate of change of costs to support the process	global measure	impl	derived

	New measures			
	number of high-value information assets categorized by high-value service (includes number of high-value assets that support more than 1, more than 2, etc. high-value services)	asset inventory	impl	base of scale ratio, type count
	percentage of high-value information assets that satisfy (that do not satisfy) their allocated resilience requirements	asset evaluation	impl; could be effectiveness	derived
	percentage of high-value information assets for which there are no (missing) protection (sustainment) controls	asset evaluation	impl; could be effectiveness	derived
	percentage of high-value information asset controls (protect, sustain) that are ineffective or inadequate as demonstrated by: • unsatisfied control objectives • unmet resilience requirements • outstanding control assessment problem areas above established thresholds/without remediation plans	asset evaluation	impl; could be effectiveness	derived

5 Defining a Process for Resilience Measurement and Analysis

This section presents several approaches for defining and implementing an effective measurement and analysis process. Such a process is required to build a sustainable capability that encompasses the objectives, measurement concepts, and examples described in the previous sections. There are many excellent and useful sources that define processes for measurement and analysis including the CERT-RMM Measurement and Analysis (MA) process area. We summarize several of the leading ones here and refer the reader to these sources for additional details. As a next step, our intent is to use all sources to possibly extend MA and to provide process definition and implementation details necessary for enacting an effective, sustainable resilience measurement and analysis activity.

The purpose of a process for measurement and analysis is to implement and sustain a measurement capability that satisfies the information needs of decision makers, providing them with the right information, at the right time, and in a form that is meaningful. For the purpose of this research, needed information is that which supports decision makers in effectively managing operational resilience, during normal operations and in times of stress and disruption.

A measurement and analysis process typically involves the following: [CMMI Product Team 2006]

- specifying the objectives for measurement and analysis such that they are aligned with identified information needs and objectives
- specifying the measures, analysis techniques, and mechanisms for data collection, data storage, reporting, and feedback
- implementing the collection, storage, analysis, and reporting of the data
- providing objective results that can be used in making informed decisions, and taking appropriate corrective actions

The types of activities generally included in a measurement and analysis process are as follows: [ISO 2007]

- establishing and sustaining commitment to the measurement program and process
- planning for measurement
- performing measurement
- evaluating the measurement process
- improving the measurement process and other processes that it informs (in satisfying information needs)

These activities and their relationships are shown in Figure 7, which is adapted from ISO/IEC 15939:2007 *Systems and Software Engineering – Measurement Process* [ISO 2007]. A version of this figure also appears in *Practical Software Measurement: Objective Information for Decision Maker*s [McGarry 2002].

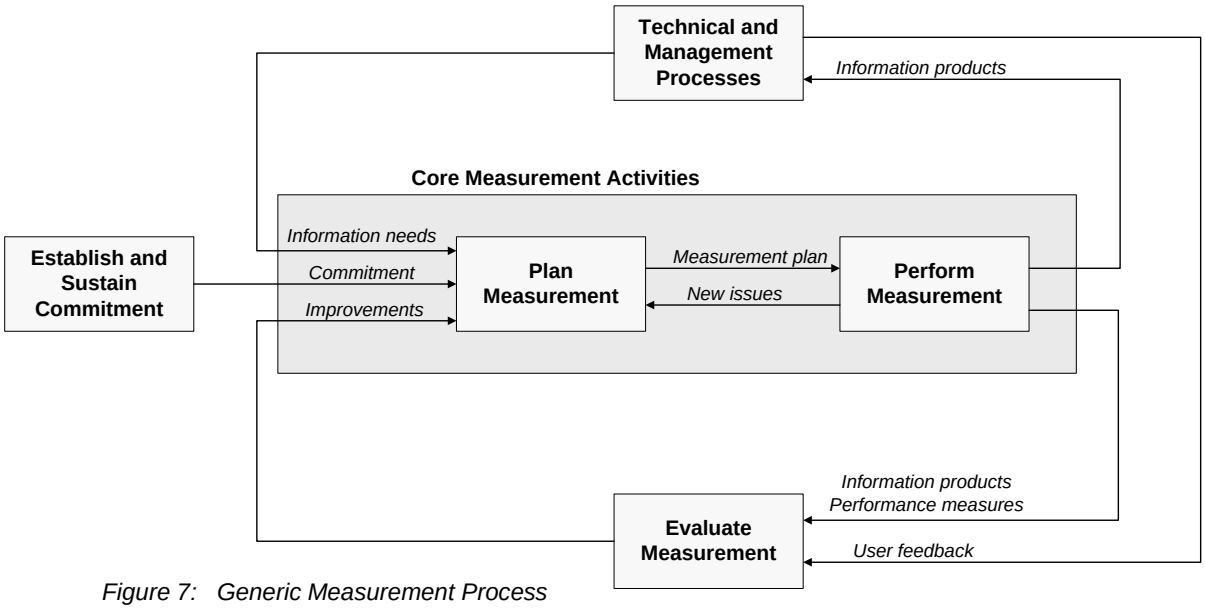


Figure 7: Generic Measurement Process

Each of the major process activities identified in Figure 7 is further elaborated in Table 23 with their corresponding ISO 15939 section numbers [ISO 2007].

Table 23: ISO 15939 Process Activities and Tasks

Activity	Task
5.1 Establish and sustain measurement commitment	5.1.1 Accept the requirements for measurement
	5.1.2 Assign resources
5.2 Plan the measurement process	5.2.1 Characterize the organizational unit
	5.2.2 Identify information needs
	5.2.3 Select measures
	5.2.4 Define data collection, analysis, and reporting procedures
	5.2.5 Define criteria for evaluating the information products and the measurement process
	5.2.6 Review, approve, and provide resources for measurement tasks
	5.2.7 Acquire and deploy supporting technologies
5.3 Perform the measurement process	5.3.1 Integrate procedures
	5.3.2 Collect data
	5.3.3 Analyze data and develop information products
	5.3.4 Communicate results
5.4 Evaluate measurement	5.4.1 Evaluate information products and the measurement process
	5.4.2 Identify potential improvements

Successful implementation of a measurement and analysis process results in the following: [ISO 2007]

- commitment for measurement is established and sustained across the organizational entity
- the information needs of decision makers, and the technical and management processes that support them, are identified

- an appropriate set of measures, driven by the information needs are identified and/or developed
- measurement activities are identified
- identified measurement activities are planned
- the required data is collected, stored, and analyzed, and the results interpreted
- information products are used to support decisions and provide an objective basis for communication
- the measurement process and measures are evaluated
- improvements are communicated to the measurement process owner

The CERT-RMM Measurement and Analysis (MA) process area tailors these generic process descriptions to measure and analyze operational resilience. Section 3.3.1 Table 12 describes the MA specific goals and practices within the context of validating the measurement template. Table 24 repeats and clarifies this content in the context of defining a process for measuring and analyzing operational resilience.

Table 24: CERT-RMM Measurement and Analysis Process Area Goals and Practices

Goals	Practices
MA:SG1 Align Measurement and Analysis Activities (with identified information needs and strategic and business objectives.)	MA:SG1.SP1 Establish Measurement Objectives (based on information needs and objectives)
	MA:SG1.SP2 Specify Measures (to meet measurement objectives)
	MA:SG1.SP3 Specify Data Collection and Storage Procedures
	MA:SG1.SP4 Specify Analysis Procedures (and procedures for reporting)
MA:SG2 Provide Measurement Results (that address identified information needs and objectives.)	MA:SG2.SP1 Collect Measurement Data (consistent with objectives)
	MA:SG2.SP2 Analyze Measurement Data (against objectives)
	MA:SG2.SP3 Store Data and Results
	MA:SG2.SP4 Communicate Results

Examples of process objectives for measuring and analyzing operational resilience include the following:

- The performance of resilience activities is being measured and regularly reported.
- Strategic operational resilience management activities are on track according to plan.
- Actions requiring management involvement are elevated in a timely manner.
- The performance of process activities is being monitored and regularly reported.
- Key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports.
- Administrative, technical, and physical controls are operating as intended.
- Controls are meeting the stated intent of the resilience requirements.
- Actions resulting from internal and external audits are being closed in a timely manner.

Resilience measurement and analysis process activities include the following:

- Specify the objectives of measurement and analysis such that they are aligned with identified information needs and objectives.
- Specify the measures, analysis techniques, and mechanisms for data collection, data storage, reporting, and feedback.
- Implement the collection, storage, analysis, and reporting of the data.
- Provide objective results that can be used in making informed decisions, and taking appropriate corrective actions.

Integrating measurement and analysis into the operational resilience management program supports

- planning, estimating, and executing operational resilience management activities
- tracking the performance of operational resilience management activities against established plans and objectives, including resilience requirements
- identifying and resolving issues in operational resilience management processes
- providing a basis for incorporating measurement into additional operational resilience management processes in the future

Readers are referred to the sources cited above and the CERT-RMM MA PA for further details [Caralli 2010a, 2010b].

6 Next Steps

Our intent is that this report serves as the first in a series on measuring and analyzing operational resilience. The purpose of measurement and analysis is to provide meaningful information for business leaders and decision makers, when they need it and in the form that they need it. A secondary purpose is to guide the day-to-day operational resilience of services and their associated assets. Measures can be used to determine the extent to which the organization is meeting its objectives for managing operational resilience (or not) as stated in Section 2. Measures can aid in addressing some of the questions raised in the Appendix. And measures can help business leaders begin to consider how to go about determining if their investments in improving their level of operational resilience are paying off.

One of the key questions we want to be able to answer in conducting this measurement and analysis research is if an organization does what is described in this report and implements this measurement approach, will it satisfy the Measurement and Analysis process area in a CERT-RMM appraisal at capability level 2?

Another concept we plan to explore involves connecting the measurement framework proposed in this report to one or more CERT-RMM-based process definitions. CERT-RMM is a process model; to implement the model, an organization will need to define more detailed, prescriptive, and implementable CERT-RMM processes in the context of the organization's ORM needs. We plan to explore the development and use of defined processes that provide opportunities for measurement and analysis at the operational level.

We also plan to develop a more prescriptive implementation guide for getting stared in measuring and analyzing operational resilience to include (but not be limited to) the following steps:

- define five to ten to fifteen objective-based measures using the templates presented in this report (or tailored as needed)
- define and assign the key roles to collect these measures
- identify initial tools to assist in data collection and analysis
- start reporting measures on a regular basis
- iterate and refine as you go
- work with the CERT-RMM User's Group to gain insights from peers and provide lessons learned

As the model is used by more organizations, it will be increasingly possible to identify, define, deploy, pilot test, and measure effective resilience measures as well as collect measurement experiences in support of benchmarking. These measures will likely be focused on implementation initially (the degree to which a practice is present or absent). We anticipate that as more organizations implement operational resilience processes, measures of effectiveness and process performance in the context of specific ecosystems will emerge. We will be working with collaborators and customers to determine what measures are most useful for evaluating effectiveness, to develop measurement templates and structured definitions, and to update the CERT-RMM to reflect

what we have learned. Automated approaches for collecting and reporting measures are essential for long term use and sustainability so these will be explored.

Appendix Resilience Questions to Drive Measurement

This appendix contains several examples of key questions that decision makers can ask to help determine their current and desired state of operational resilience for which measures can be defined and derived.

1. What organizational information needs are resilience measures and analyses intended to satisfy? What organizational decisions are resilience measures and analyses intended to inform?
    a. Have our processes made us more resilient?
    b. How resilient are we? (What should be measured to determine if performance objectives for operational resilience are being achieved?)
    c. Do we fulfill compliance obligations related to operational resilience?
2. How do I define my performance objectives and help to fulfill business objectives, mitigate risks, meet compliance requirements, assess my status against the competition, ensure that my liabilities are limited, and that my resilience management process is viable?
    a. And express them in a form that can be measured (preferably quantitatively)?
3. What is my organization's (business unit's) current level of operational resilience when compared to performance objectives?
    a. How do I know? (processes, controls, measures, meet recovery time objectives (RTO)/recovery point objectives (RPO), service continuity plans in place/tested)
    b. How do I express, describe, and report this?
    c. How do I compare to my peers/competitors?
4. How well are we performing today?
    a. Can we repeat our successes?
    b. Do we consistently produce expected results?
    c. Can we adapt seamlessly to changing risk environments?
    d. Are our processes stable enough to depend on them under times of stress?
    e. Can we predict how we will perform under times of stress?
5. How do I prioritize the investments necessary to move from my current state to the state required to fulfill my performance objectives?
    a. What are the prioritization criteria?
6. How do I know if I'm making progress as expected?
    a. What should be measured to determine if performance objectives are being achieved (are being sustained)?
    b. How do I know if I am at least sustaining my current state while moving toward fulfilling all performance objectives?
    c. How do I ensure that I am allocating budget to the highest priority investments?

7. How do I determine the effectiveness of/the contribution of (selected, aggregate) resilience processes in improving/sustaining operational resilience?
    a. Adapt seamlessly to changing risk environments.
    b. Perform predictably under times of stress.
    c. Informed by MA and MON PAs.
8. What is the cost to the organization for not taking a process improvement/maturity approach to managing operational resilience?
9. Who pays for poor operational resilience processes? What cost is there to customers, share-holders, employees, and the community?
10. Who owns the "quality" challenge for operational resilience processes? How do they define and measure quality?
11. What is the value to an organization of stabilizing operational resilience processes?

Glossary of Terms

Adequate
Commensurate in fitness; equal or amounting to what is required; fully sufficient, suitable, or fitting.[33]

Adherence
Persistence in a practice or tenet; steady observance or maintenance.[34]

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

Asset
Something of value to the organization, typically, people, information, technology, and facilities that high-value services rely on. [ADM]

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

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]

Effective
Producing a decided, decisive, or desired effect (result)[35]

Efficient
An acting or a potential for action or use in such a way as to avoid loss or waste of energy in effecting, producing, or functioning[36]

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

[33] http://www.oed.com/

[34] http://www.oed.com/

[35] http://www.merriam-webster.com/

[36] http://www.merriam-webster.com/

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

High-value service
Services on which the success of the organization's mission depends. [EF] [RRD]

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

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 the related term *operational risk*.)

Operational resilience management
The direction and coordination of activities to achieve resilience objectives that align with the organization's strategic objectives and critical success factors.

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.

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 the related term *organizational unit*).

Organizational drivers
Drivers include strategic objectives, critical success factors, strategic resilience requirements, compliance obligations, and so forth.

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

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 the related term *condition*).

Realized risk
Operational disruption due to an incident, disaster, or other disruptive event (see also *risk*).

Risk
The possibility of suffering harm or loss. From a resilience perspective, risk is the combination of a threat and a vulnerability (condition), the impact (consequence) on the organization if the vulnerability is exploited, and the presence of uncertainty. 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 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 the related terms *area of impact*, *risk measurement criteria*, and *risk tolerance*).

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

Risk 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 the related terms *risk tolerance* and *risk measurement criteria*).

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 has 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]

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 the related term *business process*).

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.

Acronyms

CERT-RMM Process Areas (PAs)

Enterprise Process Areas

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

Engineering Process Areas

- ADM - Asset Definition and Management
- RRD - Resiliency Requirements Development
- RRM- Resiliency Requirements Management
- CTRL - Controls Management
- RTSE - Resilient Technical Solution Engineering
- SC - Service Continuity

Operations Management Process Areas

- EC - Environmental Control
- KIM – Knowledge & Information Management
- PM – People Management
- TM – Technology Management
- AM – Access Management
- ID – Identity Management
- IMC – Incident Management & Control
- VAR – Vulnerability Analysis & Resolution
- EXD – External Dependencies

Process Management Process Areas

- MON – Monitoring
- MA – Measurement and Analysis
- OPD – Organizational Process Definition
- OPF – Organizational Process Focus

Other Acronyms

CISO – Chief Information Security Officer

CRM – Customer Relationship Management

CSIRT – Computer Security Incident Response Team

GQ(I)M – Goal Question (Indicator) Metric

GQM – Goal Question Metric

HR – Human Resources

ORM – Operational Resilience Management

ORPG – Operational Resilience Process Group

SEPG – Software Engineering Process Group

References/Bibliography

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

[Bartol 2008]
Bartol, Nadya. *Practical Measurement Framework for Software Assurance and Information Security, Version 1.0*. Practical Software & Systems Measurement (PSM), 2008. http://www.psmsc.com/Prod_TechPapers.asp.

[Basili 1984]
Basili, Victor R. and Weiss, David M. "A Methodology for Collecting Valid Software Engineering Data." IEEE Transactions on Software Engineering, Vol. SE-10, No. 6, November 1984. http://www.cs.umd.edu/~basili/publications/journals/J23.pdf

[Basili 1988]
Basili, Victor R. & Rombach, H. Dieter. "The TAME Project: Towards Improvement-Oriented Software Environments." IEEE Transactions on Software Engineering, Vol. 14, No. 6 (June 1988): 758-773.

[Basili 1994]
Victor R. Basili, Gianluigi Caldiera, H. Dieter Rombach}, *The Goal Question Metric Approach,* Encyclopedia of Software Engineering, Wiley 1994

[BSI 2006]
The British Standards Institution. *BS 25999: Business Continuity Management, Part 1: Code of Practice*. BSI, November 2006 (ISBN 0 580 49601 5). www.bsigroup.com

[Caralli 2010a]
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

[Caralli 2010b]
Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; & Young, Lisa R. *CERT® Resilience Management Model, v1.0 - Process Areas, Generic Goals and Practices, and Glossary (CERT-RMM v1.0).* Software Engineering Institute, Carnegie Mellon University, 2010. http://www.cert.org/resilience/rmm.html

[Caralli 2010c]
Caralli, Richard A., et al. "Improving Operational Resilience Processes: The CERT Resilience Management Model." Conference proceedings for the Second IEE International Conference on Privacy, Security, Risk, and Trust (PASSAT2010); Workshop on Mission Assurance: Tools, Techniques, and Methods. Minneapolis, Minnesota. August 20-22, 2010.

[Caralli 2010d]
Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; & Young, Lisa R. *CERT® Resilience Management Model, v1.0 - Glossary of Terms*. Software Engineering Institute, Carnegie Mellon University, 2010. http://www.cert.org/resilience/rmm.html

[CISWG 2005]
Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. "Report of the Best Practices and Metrics Teams." November 17, 2004; updated January 10, 2005.
http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661

[CMMI Product Team 2006]
CMMI Product Team. *CMMI® for Development, Version 1.2* (CMU/SEI-2006-TR-008). Software Engineering Institute, Carnegie Mellon University, 2006.
http://www.sei.cmu.edu/library/abstracts/reports/06tr008.cfm

[ITGI 2007]
IT Governance Institute. *COBIT 4.1*. Rolling Meadows, IL: ITGI, 2007. www.isaca.org

[Deming 1986]
Deming, W. Edwards. *Out of the Crisis*. MIT Center for Advanced Educational Services, Cambridge, MA 1986.

[DRJ 2006]
DRJ Editorial Advisory Board Generally Accepted Business Continuity Practices Committee and DRI International. *Generally Accepted Practices For Business Continuity Practitioners*. Disaster Recovery Journal and DRII, August 2007. http://www.drj.com/GAP/gap.pdf

[Fenton 1991]
Fenton, Norman E. *Software Metrics: A Rigorous Approach*. London: Chapman & Hall, 1991.

[Fenton 1995]
Fenton, Norman E. & Whitty, Robin. "Introduction," 1-19. *Software Quality Assurance and Measurement, A Worldwide Perspective*, Norman Fenton, Robin Whitty, and Yoshinori Iizuka, ed. London: International Thomson Computer Press, 1995.

[FFIEC 2008]
Federal Financial Institutions Examination Council. "Business Continuity Planning." *IT Examination Handbook*. FFIEC, March 2008.
http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf

[Ghiselli 1981]
Ghiselli, Edwin E.; Campbell, John P.; & Zedeck, Sheldon. *Measurement Theory for the Behavioral Sciences*. San Francisco, Calif.: W. H. Freeman and Company, 1981.

[Goethert 2001]
Goethert, Wolfhart Goethert & Hayes,Will. *Experiences in Implementing Measurement Programs* (CMU/SEI-2001-TR-026). Software Engineering Institute, Carnegie Mellon University, 2001. http://www.sei.cmu.edu/reports/01tn026.pdf

[Hubbard 2007]
Hubbard, Douglas. *How to Measure Anything*. Wiley , 2007.

[ISO 2005]
International Organization for Standardization. *Information technology – Security techniques – Code of practice for information security management*. ISO/IEC 27002:2005, June 2005. Also known as ISO/IEC 17799:2005.

[ISO 2007]
International Organization for Standardization. *Systems and software engineering – Measurement process, second edition*. ISO/IEC 15939:2007, August 2007.

[Krantz 1971]
Krantz, David H.; Luce, R. Duncan; Suppes, Patrick; & Tversky, Amos. *Foundations of Measurement*, Vol.1. New York, N.Y.: Academic Press, 1971.

[McGarry 2002]
McGarry, John, et. al. *Practical Software Measurement: Objectives for Decision Makers*. Addison-Wesley, 2002.

[McGraw 2010]
McGraw, Gary; Chess, Brian; & Migues, Sammy. *Building Security In Maturity Model BSIMM v2.0*. http://www.bsimm2.com/ (Accessed July 2010).

[Mills 1988]
Mills, Everald E. "Software Metrics, SEI Curriculum Module SEI-CM-12-1.1." Carnegie Mellon University, Software Engineering Institute, 1988.

[NIST 2008]
Chew, Elizabeth; Swanson, Marianne; Stine, Kevin; Bartol, Nadya; Brown, Anthony; & Robinson, Will. *Performance Measurement Guide for Information Security*. NIST Special Publication 800-55, Revision 1. Gaithersburg, MD: National Institute of Standards and Technology, July 2008. http://csrc.nist.gov/publications/PubsSPs.html

[Park 1996]
Park, Robert; Goethert, Wolfhart; Florac, William. *Goal-Driven Software Measurement —A Guidebook.* Handbook CMU/SEI-96-HB-002. Carnegie Mellon University: Software Engineering Institute, 1996.

[PSM 2010]
Practical Software and Systems Measurement web site. http://www.psmsc.com/

[REF Team 2008]
Resiliency Engineering Framework Team. *CERT Resiliency Engineering Framework: Code of Practice Crosswalk, Preview Version, V0.95R*. Software Engineering Institute, Carnegie Mellon University, 2008. http://www.cert.org/resilience/rmm_materials.html

[Roberts 1979]
Roberts, Fred S. *Measurement Theory with Applications to Decisionmaking, Utility, and the Social Sciences*. Reading, Mass.: Addison-Wesley, 1979.

[Rombach 1989]
Rombach, H. Dieter & Ulery, Bradford T. "Improving Software Maintenance Through Measurement." Proceedings of the IEEE, Vol. 77, No. 4 (April 1989): 581-595.

[SEMA 2010]
Software Engineering Institute Software Engineering Measurement and Analysis web site. http://www.sei.cmu.edu/measurement

[SSE-CMM 2003]
Systems Security Engineering Capability Maturity Model Model Description Document, Version 3.0. 2003. http://www.sse-cmm.org/model/model.asp

[Stevens 1946]
Stevens, S. S. "On the Theory of Scales of Measurement." Science, Vol. 103, No. 2684 (1946): 677–680.

[Stevens 1951]
Stevens, S. S. "Mathematics, Measurement, and Psychophysics," 1–49. Handbook of Experimental Psychology, S. S. Stevens, ed. New York, N.Y.: John Wiley & Sons, Inc., 1951.

[Stevens 1959]
Stevens, S. S. "Measurement, Psychophysics, and Utility," 18–63. *Measurement: Definitions and Theories*, C. West Churchman & Philburn Ratoosh, ed. New York, N.Y.: John Wiley & Sons, Inc., 1959.

[Wheeler 2000]
Wheeler, Donald J. *Understanding Variation: The Key to Managing Chaos, Second edition*. SPC PRESS (Statistical Process Control), 2000.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	September 2010	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Measuring Operational Resilience Using the CERT® Resilience Management Model	FA8721-05-C-0003

6. AUTHOR(S)

Julia H. Allen & Noopur Davis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2010-TN-030

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

Measurement involves transforming management decisions, such as strategic direction and policy, into action, and measuring the performance of that action. As organizations strive to improve their ability to effectively manage operational resilience, it is essential that they have an approach for determining what measures best inform the extent to which they are meeting their performance objectives. Operational resilience comprises the disciplines of security, business continuity, and aspects of IT operations.

The reference model used as the foundation for this research project is the CERT® Resilience Management Model v1.0. This model provides a process-based framework of goals and practices at four increasing levels of capability and defines twenty six process areas, each of which includes a set of candidate measures. Meaningful measurement occurs in a context so this approach is further defined by exploring and deriving example measures within the context of selected ecosystems, which are collections of process areas that are required to meet a specific objective. Example measures are defined using a measurement template.

This report is the first in a series and is intended to start a dialogue on this important topic.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Resilience management, risk, measure, measurement	83

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