Software Engineering Institute

Measures for Managing Operational Resilience

Julia H. Allen
Pamela D. Curtis

July 2011

TECHNICAL REPORT
CMU/SEI-2011-TR-019
ESC-TR-2011-019

CERT® Program

http://www.sei.cmu.edu

Carnegie Mellon

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

This report was prepared for the

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

For information about SEI publications, please visit the library on the SEI website (www.sei.cmu.edu/library).

Table of Contents

Acknowledgments

The authors would like to thank the reviewers of this report for their thoughtful and valuable comments. Reviewers are members of the CERT Resilient Enterprise Management Team.

- Rich Caralli
- Jim Cebula
- John Haller
- Sam Merrell
- Kevin Partridge
- Barbara Tyson
- David White
- Lisa Young

The authors would also like to thank Noopur Davis of Davis Systems for her review comments. Noopur regularly contributes to REM team measurement work and is the co-author of *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010].

Abstract

How resilient is my organization? Have our processes made us more resilient? Members of the CERT® Resilient Enterprise Management (REM) team are conducting research to address these and other related questions. The team's first report, Measuring Operational Resilience Using the CERT Resilience Management Model, defined high-level objectives for managing an operational resilience management (ORM) system, demonstrated how to derive meaningful measures from those objectives, and presented a template for defining resilience measures, along with example measures.

In this report, REM team members suggest a set of top ten strategic measures for managing operational resilience. These measures derive from high-level objectives of the ORM system defined in the CERT® Resilience Management Model, Version 1.1 (CERT®-RMM). The report also provides measures for each of the 26 process areas of CERT-RMM, as well as a set of global measures that apply to all process areas. This report thus serves as an addendum to CERT-RMM Version 1.1.

Since CERT-RMM practices map to bodies of knowledge and codes of practice such as ITIL, COBIT, ISO2700x, BS25999, and PCI DSS, the measures may be useful for measuring security, business continuity, and IT operations management processes, either as part of adoption of CERT-RMM or independent of it.

1 Introduction

The purpose of this technical report is to present operational resilience measures developed through ongoing research that was first reported in *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010].

CERT®-RMM[1] version 1.1 defines 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" [Caralli 2011].

Operational risk management is supported and enabled by the disciplines of security, business continuity, and some aspects of IT operations. CERT-RMM provides a process view of resilience by describing the practices of these disciplines as part of larger enterprise processes. A process can be defined, communicated, and controlled. The desired goals and outcomes of the process can be identified, success in reaching those goals and outcomes can be measured, and gaps can be identified and addressed.

Operational resilience supports the ability of services and their associated assets (information, technology such as systems and software, facilities, and people) 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[2] or stress is eliminated. A service is *not* resilient if it cannot return to normalcy after being disrupted, even if it can temporarily withstand adverse circumstances.

Resilience objectives for services and assets are achieved through an *operational resilience management (ORM) system*. An ORM system includes all of the processes necessary to manage operational resilience, along with their associated and supporting plans, programs, procedures, practices, and people. In our first report, we defined high-level objectives for managing an ORM system and demonstrated how to derive meaningful measures from those objectives. For example, one high-level objective identified was, "Demonstrate that the ORM system sustains high-value services and associated assets during and following a disruptive event." One measure defined for that objective was, "For disrupted high-value services with a service continuity plan, percentage of services that delivered service as intended throughout the disruptive event" [Allen 2010].

Linking to high-level objectives can help establish measurement priorities at the enterprise level. Some strategic measures provide meaningful information for business decision making, and many can be used to guide the day-to-day operational resilience of services and their associated assets. In Chapter 2 of this report, we take another look at deriving measures from high-level objectives to suggest a list of the top ten strategic measures for managing operational resilience.

[1] CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

[2] "Disruption" in this definition applies to a disturbance that does not exceed the service's operational limit. A catastrophic loss of infrastructure would not be considered a disruption.

1.1 Process Area Measures

The bulk of this report, however, focuses on measurement priorities for each of the 26 CERT-RMM process areas (PAs).[3] These measures were derived from the specific practices and subpractices of the PAs and are intended to measure either the extent of the practices' implementation or their effectiveness in improving operational resilience.

Some of the measures appear in simple list form in Generic Goal 2, Generic Practice 8 (GG2.GP8), "Monitor and Control the Process," in their respective PAs in Version 1.1 of the model, and they are updated and expanded in this report. Other measures are new as of this report. They are process measure examples for GG2.GP8 subpractice 2, "Review accomplishments and results of the process against the plan for performing the process."[4] The generic goals and practices in the model are those that apply to every PA; thus every PA has a GG2.GP8, but the measure examples are specific to each PA.

The generic goals and practices in CERT-RMM are indicators of progressive levels of capability. Generic goal 1 in any PA relates to achieving performance of the specific practices of that PA (capability level 1). Generic goal 2 assumes that the specific practices are being performed and provides guidance for higher capability practices such as planning the process and measuring performance against the plan. For those who are using the model, the measures can be used to help achieve capability level 2 in any given PA. For those who are *not* using the model, the measures can be useful for measuring security, business continuity, and IT operations management processes because CERT-RMM practices map to bodies of knowledge and codes of practice such as ITIL, COBIT, ISO2700x, BS25999, and PCI DSS.

We expect many of these tactical measures at the PA level will be combined to inform more strategic measures, which will in turn demonstrate the extent to which operational resilience objectives are (or are not) being met. So there is a need for both types of measures.

1.2 Information Needs That Drive Resilience Measurement

The measures in this report result from research by the authors and other CERT Program staff members at the SEI to assist business leaders in addressing key questions they may be asked (or may ask themselves). The measures inform the answers to these questions:

- How resilient is my organization?
- Is it resilient enough?
- How resilient does it need to be?

Some further interpretations of these questions might include the following:

- Do I need to worry about operational resilience?

---

[3] A process area is a cluster of related practices in an area that, when implemented collectively, satisfies a set of goals considered essential for that area. For example, the goals of the CERT-RMM People Management PA are "Establish Vital Staff," "Manage Risks Associated with Staff Availability," and "Manage the Availability of Staff."

[4] Although the authors have attempted to be thorough in developing useful measures related to the CERT-RMM PAs, there may be other measures that will be meaningful for your organization. *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010] provides guidance and a template for developing resilience measures.

- If my services are disrupted, will it make the news? Will I end up in court? In jail? Will I be able to stay in business?
- Do I meet compliance requirements?
- How resilient am I compared to my competition?
- Do I need to spend more on resilience? If so, on what?
- What am I getting for what I've already spent?
- What is the business value of being more resilient?

The key questions being addressed by this research project include

- What should I be measuring to determine if I am achieving my performance objectives for operational resilience?
- Have our processes made us more resilient?
- Given that measurement is expensive, how can I identify measures that will most effectively inform decisions and affect behavior?

1.3 Report Overview

As mentioned above, Chapter 2 of this technical report introduces a set of "top ten" strategic measures that have been derived from the objectives for operational resilience in *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010]. These measures have received positive feedback at several conferences. We will continue to update and refine these measures as the basis for additional measures that provide a top-down view.

The Appendix of this report updates all process implementation and effectiveness measures listed in Generic Goal 2, Generic Practice 8 (GG2.GP8), "Monitor and Control the Process," in each of the 26 PAs of CERT-RMM v1.1. These process implementation and effectiveness measures provide a bottom-up, tactical view.

The purpose of this update is to improve completeness (with respect to covering the specific goals and practices in CERT-RMM v1.1), consistency, and clarity. In addition, the report adds a new set of global measures that apply to all PAs. These global measures have been deleted from each of the individual PAs. The tables presented in this report serve as updates and an addendum to CERT-RMM v1.1 and replace corresponding elaboration tables in GG2.GP8 subpractice 2 for each PA.

Some of the measures use concepts and terminology from the model. Please refer to the glossary and relevant PA sections in CERT-RMM ([Caralli 2011] or www.cert.org/resilience/rmm.html) for clarification as needed.

2 Top Ten Strategic Measures

Operational resilience strategic measures help ensure that any measurement of operational resilience directly supports the achievement of business objectives. One of the many pitfalls of unsuccessful measurement programs is collecting, analyzing, and reporting data that does not contribute to informing decisions or changing behavior. Often measurement programs collect and report measures of "type count" (such as number of incidents, number of systems with patches installed, number of people trained) with little meaningful context for how these measures will be used.[5] By having a set of strategic measures, we can map those measures to the most useful measures at the individual PA level and develop criteria to determine which PA-level measures best address the questions posed in the Introduction. In addition, measurement can be expensive, and organizations should be judicious in selecting measures that form the foundation of their measurement program.

The strategic objectives for an ORM system are described in the next five sections. Each is currently supported by two measures. For further details, refer to Section 2.3 of *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010].

2.1 Organizational Objectives

Objective: The ORM system derives its authority from and directly traces to organizational drivers. Organizational drivers include strategic objectives and critical success factors (refer to the Enterprise Focus process area [Caralli 2011]). An alternative way of stating this might be "The ORM system derives its authority from a directive given by a senior, high-level executive." This could be considered one form of organizational driver.

Measure 1: Percentage of resilience activities that do not directly (or indirectly) support one or more organizational objectives. An activity can be a project, task, performance objective, or investment, and represents some meaningful decomposition of the resilience program.

Measure 2: For each resilience activity, number of organizational objectives that require it to be satisfied (goal is = or > 1)

Supporting measures that address the relationship between organizational objectives and resilience are contained in the Appendix table for Enterprise Focus (EF).

2.2 High-Value Services and Assets

Objective: The ORM system satisfies resilience requirements that are assigned to high-value services and their associated assets. An alternative way of stating this might be "The ORM system satisfies governance, compliance, policy, framework, assessment, and reporting requirements." These could all be considered expressions of enterprise resilience requirements.

[5] While readers of this report will see measures of this type in the Appendix, they are presented in the context of one or more process areas and are often used as the basis for calculating derived measures.

Measure 3: Percentage of high-value services that do not satisfy their assigned resilience requirements. (Operational resilience requirements are a derivation of the traditionally described security objectives of confidentiality, availability, and integrity. They may also include privacy requirements.) A companion measure would be to measure a specific service of interest, ensuring that criteria for selecting such a service are defined.

Measure 4: Percentage of high-value assets (information, technology, facilities, and people) that do not satisfy their assigned resilience requirements. Examples of assets are network infrastructure, a specific application, a database, a data center, and a lead system administrator.

Supporting measures that address resilience requirements for services are contained in the Appendix table for EF. Supporting measures that address resilience requirements for assets are contained in the following Appendix tables by asset type:

- Asset Definition and Management (ADM) – general
- Environmental Control (EC) – facilities
- Knowledge Information and Management (KIM) – information
- People Management (PM) – people
- Technology Management (TM) – technology

2.3 Controls

Objective: Via the internal control system,[6] the ORM system ensures that controls for protecting and sustaining high-value services and their associated assets operate as intended.

Measure 5: Percentage of high-value services with controls that are ineffective or inadequate. This may include unsatisfied control objectives, unmet resilience requirements, missing controls, and outstanding assessment and audit problems above threshold without remediation plans.

Measure 6: Percentage of high-value assets with controls that are ineffective or inadequate

Supporting measures that address controls in general are contained in the Appendix table for Controls Management (CTRL). Supporting measures that address controls for assets are contained in the Appendix tables by asset type as noted in Section 2.2, Measure 4.

2.4 Risks

Objective: The ORM system manages operational risks to high-value assets that could adversely affect the operation and delivery of high-value services.

Measure 7: Confidence factor that risks from all sources that need to be identified have been identified. A detailed template for this measure appears in Section 4.1.1 of *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010].

Measure 8: Percentage of risks with impact above threshold. This should include risks without mitigation plans, risks that are not effectively mitigated by their mitigation plans, and risks that have not been reviewed in the required time frame.

[6] The internal control system includes the methods, policies, and procedures used to protect and sustain assets at a level commensurate with their role in supporting high-value services.

Supporting measures that address risks in general are contained in the Appendix table for Risk Management (RISK). Supporting measures that address risks for assets are contained in the Appendix tables by asset type as noted in Section 2.2, Measure 4.

2.5 Disruptive Events

Objective: In the face of realized risk, the ORM system ensures the continuity of essential operations of high-value services and their associated assets. Realized risk may include an incident, a break in service continuity, or a man-made or natural disaster or crisis.

Measure 9: Probability of delivered service through a disruptive event

Measure 10: For disrupted, high-value services with a service continuity plan, percentage of services that did not deliver service as intended throughout the disruptive event

Consider using "near misses" and "incidents avoided" as predictors of successful disruptions in the future.

Supporting measures that address service continuity are contained in the Appendix table for Service Continuity (SC). Supporting measures that address incident management are contained in the Appendix table for Incident Management and Control (IMC).

3 Introduction to the Resilience Measures

The following process was used to generate the tables of resilience measures presented in the Appendix:

1. Starting with existing GG2.GP8 subpractice 2 process area measures for each PA in CERT-RMM v1.1, the type of information that each measure addresses was designated (see the Column 3 description below). Measures were then ordered in a logical progression by type of information.
2. The new Measure Type and Base or Derived columns (Columns 4 and 5, respectively) were populated for each existing measure.
3. The PA specific goals and specific practices were carefully reviewed, and measures were added, corrected, combined, or eliminated, as needed. Each measure was mapped to the specific goal(s) and practice(s) that it informs (Column 6).
4. All measures were edited for clarity and consistency and to eliminate redundancy, separate compound measures, and eliminate measures of insufficient information value.
5. Measures that are global in nature were identified (that is, ones that apply to all PAs). A new table of global measures was created, and the global measures were deleted from the tables of PA-specific measures. Global measures were defined for the generic goals and practices that accompany each process area.
6. All measures tables were reviewed by at least two reviewers.

This process was started for three process areas in *Measuring Operational Resilience Using the CERT Resilience Management Model*, specifically Knowledge and Information Management (KIM), Incident Management and Control (IMC), and Risk Management (RISK). Refer to Section 4.1 of that document for information on these three process areas in the context of selected CERT-RMM ecosystems (a collection of process areas, relationships, goals, and practices that contribute to a specific objective, such as the management of risk).

Each table is organized as follows (refer to the Appendix):

Column 1: ID

The ID field is a unique, sequential identifier that is assigned to each measure. We organized measures in a logical progression, which often matches the order of the specific goals and practices for the specific PA. The Column 3 entry typically determines the order of the measures.

Column 2: Measure

This field contains the measure or, in some cases, a set of related measures.

Column 3: Type of Information

The intent of this field is to identify several standard types of information within each PA that the measure informs. These may be CERT-RMM work products (such as asset inventory and asset controls) or activities (such as change management and obligation satisfaction). Type of informa-

tion entries support some level of affinity grouping of related measures and may be used in the future to reduce or aggregate related measures.

Column 4: Measure Type

Measures can be one of three types:

- *Implementation* measures answer the question, Is this process, activity, or practice being performed? Such measures provide no information regarding the contribution (or lack thereof) that the activity is making to improved operational resilience. The measures presented in this report are predominantly implementation measures. This is as expected for this stage of our research project, given that such measures describe an organization's behavior as it is starting to improve its operational resilience management processes (referred to in CERT-RMM as capability levels 1 and 2).
- *Effectiveness* measures answer the questions, How good is the work product or outcome of the process, activity, or practice? Does it achieve the intended result? Effectiveness measures are typically of much greater interest than implementation ones. Many of them derive from one or more implementation measures.
- *Process performance* measures answer the questions, Is the process performing as expected? Is it efficient? Can it be planned? Is it predictive? Is it in control? There are only a few process performance measures described in this report. This is as expected for this stage of our research project, given that organizations focus on institutionalizing defined processes at a later stage of their resilience improvement activities (referred to in CERT-RMM as capability level 3).

On occasion, the Measure Type field states "implementation, possibly effectiveness." Such measures may be potential candidates for effectiveness measures but require additional interpretation and analysis.

For further details on these definitions, refer to Section 3.1.3 of *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010].

Column 5: Base or Derived

This field indicates whether the measure is a base measure or a derived measure, defined as follows:

- A base measure is a directly observable attribute of an asset, service, or resilience process. 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 can be measured in days or months. A base measure is thus defined by fundamental units that are not composed of any other units and is functionally independent of other measures. Base measures can be one of four types: count, cost or effort, schedule, or defects. Most of the base measures presented in the tables are of type count (number of) or of type schedule (elapsed time since or total calendar time).
- A derived measure is a mathematical function of two or more base and/or derived measures. Examples of resilience derived measures are percentage of incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds; percentage of information as-

sets without assigned resilience requirements; and change in number of identified risks that exceed risk parameters.

For further details on these definitions, refer to Section 3.1 of *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010].

Column 6: Applicable SG.SP

This field contains the mapping of the measure to applicable CERT-RMM specific goals and practices. The identified SGs and SPs served as the source for the measure. Occasionally the field entry states "none." This indicates a measure that derives from another source (such as a CERT-RMM appraisal) and is not specifically called for in the model.

While the tables are presented in alphabetical order by PA acronym, measures were often developed across related sets of PAs that share common specific goals and practices. Three noteworthy "clusters" of PAs are the asset cluster, the risk cluster, and the controls cluster. Readers of the measures contained in these tables will see commonality and repetition of certain measures. While repetition adds to the effort to maintain measures tables, we want to ensure that each table stands alone to the greatest extent possible (without having to draw upon measures in other PA tables). These clusters include the following process areas:

- **Asset cluster**: This cluster includes the following related process areas for the identification and management of assets:
  - ADM: Asset Definition and Management
  - EC: Environmental Control
  - KIM: Knowledge and Information Management
  - PM: People Management
  - TM: Technology Management

  A number of measures that appear in ADM are repeated in EC, KIM, PM, and TM, qualified by asset type (facilities, information, people, and technology, respectively).

- **Risk cluster**: This cluster includes the following related process areas for the identification and management of risks to assets:
  - RISK: Risk Management
  - EC: Environmental Control
  - KIM: Knowledge and Information Management
  - PM: People Management
  - TM: Technology Management

  This cluster also includes the External Dependencies (EXD) PA for the identification and management of risks to external entities and external dependencies. A number of measures that appear in RISK are repeated in EC, KIM, PM, and TM as well as EXD.

- **Controls cluster**: This cluster includes the following related process areas for the identification and management of controls for assets:
  - CTRL: Controls Management

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

A number of measures that appear in CTRL are repeated in EC, KIM, PM, and TM, qualified by asset type (facilities, information, people, and technology, respectively).

All measures are intended to be repeatedly collected and reported over time. Often changes in measures from one reporting period to the next and trends over time are of greatest interest. Thus, readers will not see specific references to time durations or periods of time in these measures other than the occasional use of "elapsed time."

4 Future Plans

This research project will continue through FY12 (October 2011 through September 2012). Future plans include populating a database with all of the measures identified in this report. Through use of this database, measures can be easily maintained and mapped to other CERT-RMM artifacts such as specific goals and practices and CERT-RMM Compass questions.[7]

The research team will perform the following tasks to identify additional measures and updates to existing measures:

- Review CERT-RMM appraisal results, Compass review results, and results of other CERT-RMM assessment efforts.
- Develop an approach (and templates) for defining CERT-RMM processes at the implementation level and use these process definitions to define additional measures.
- Perform a review and analysis of all measures of measure type effectiveness to identify gaps.
- Identify which process area measures provide information supporting the top ten strategic measures. Identify criteria for prioritizing process measures based on strategic measures.
- Obtain guidance and feedback from members of the CERT-RMM Users Group.

The team will also develop additional measures templates for key measures (refer to Section 3.3 of *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010]).

The authors of this report welcome your comments and feedback. We can be contacted at jha@cert.org and pdc@cert.org.

[7] http://www.cert.org/resilience/rmm_compass.html

Appendix Resilience Measures

The table of global measures that applies to all process areas appears first. It is following by 26 tables of process-area-specific measures. Each table of measures is preceded by the name of the process area, its purpose, and a summary of its specific goals and practices. This content is taken directly from the *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience* [Caralli 2011].

Global Measures

Organizations deploy generic goals and practices to attain successively improving degrees of process institutionalization and capability maturity for operational resilience management. These practices exhibit the organization's commitment and ability to perform operational resilience management processes, as well as its ability to measure performance and verify implementation.

Summary of Generic Practices for Generic Goal 2 Institutionalize a Managed Process

GG2.GP1 Establish Process Governance

GG2.GP2 Plan the Process

GG2.GP3 Provide Resources

GG2.GP4 Assign Responsibility

GG2.GP5 Train People

GG2.GP6 Manage Work Product Configurations

GG2.GP7 Identify and Involve Relevant Stakeholders

GG2.GP8 Monitor and Control the Process

GG2.GP9 Objectively Evaluate Adherence

GG2.GP10 Review Status with Higher-Level Managers

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable GG.GP
G-M1	percentage of higher-level managers who have documented resilience objectives that are reviewed as part of the normal performance review process	governance	impl	derived	GG2.GP1 GG2.GP8
G-M2	elapsed time since resilience-related compliance obligations were reviewed by higher-level managers	governance	impl	derived	GG2.GP1 GG2.GP8
G-M3	elapsed time since resilience-related controls in the context of the organization's internal control system were reviewed by higher-level managers	governance; status	impl	derived	GG2.GP1 GG2.GP8 GG2.GP10
G-M4	elapsed time since higher-level managers reviewed the priorities of services and associated assets and provided updated guidance	governance; status	impl	derived	GG2.GP1 GG2.GP8 GG2.GP10

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable GG.GP
G-M5	elapsed time since audit reports on resilience-related controls in the context of the organization's internal control system were reviewed by appropriate committees	governance; status	impl	derived	GG2.GP1 GG2.GP8 GG2.GP10
G-M6	elapsed time since higher-level managers reviewed the performance and effectiveness of the operational resilience management system and its processes and provided any necessary course correction	governance; status	impl	derived	GG2.GP1 GG2.GP8 GG2.GP10
G-M7[8]	percentage of policies[9] that are met (no violations, all exceptions approved)	policy	impl	derived	GG2.GP1 GG2.GP8
G-M8	percentage of policies (and/or procedures) that require updates to reflect CERT-RMM process area goals and practices	policy	impl	derived	GG2.GP1 GG2.GP8
G-M9	percentage of CERT-RMM practices (based on a specific model scope[10]) that are required as a result of policies (and/or procedures)	policy	impl	derived	GG2.GP1 GG2.GP8
G-M10	number of policy violations, aggregate and by policy	policy	impl	base of type count	GG2.GP1 GG2.GP8
G-M11	percentage of policy exceptions approved, aggregate and by policy	policy	impl	derived	GG2.GP1 GG2.GP8
G-M12	percentage of process activities that are on track per plan	process plan; process activities	impl	derived	GG2.GP2 GG2.GP8
G-M13	difference in planned versus actual schedule to perform the process	process plan; process activities	impl; possibly process performance	derived	GG2.GP2 GG2.GP8
G-M14	percentage of process activities approved but not implemented (due to, for example, schedule and resource constraints)	process plan; process activities	impl	derived	GG2.GP2 GG2.GP8
G-M15	number of scope changes to process activities	process plan; process activities	impl	base of type count	GG2.GP2 GG2.GP8
G-M16	change in resource needs to support the process	process plan; resources	impl; possibly effectiveness	derived	GG2.GP3 GG2.GP8
G-M17	percentage of process activities for which funds have been allocated as planned	process plan; resources	impl	derived	GG2.GP3 GG2.GP8
G-M18	percentage of process activities for which staff have been allocated as planned	process plan; resources	impl	derived	GG2.GP3 GG2.GP8
G-M19	difference in planned versus actual staff trained to perform the process	process plan; resources	impl; possibly process performance	derived	GG2.GP3 GG2.GP8
G-M20	cost to support the process	process plan; resources	impl; possibly effectiveness	derived	GG2.GP3 GG2.GP8
G-M21	difference in planned versus actual cost to perform the process	process plan; resources	impl; possibly process performance	derived	GG2.GP3 GG2.GP8

[8] Measures referring to other types of policies specific to a PA are included in the PA measures table.

[9] Policies as used here refer to new and updated organizational policies that reflect the intent of CERT-RMM process areas goals and practices.

[10] Organizations are able to select specific goals (SGs) and specific practices (SPs) from CERT-RMM that support their organizational resilience objectives.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable GG.GP
G-M22	percentage of process activities that do not have the necessary methods, techniques, and tools to support them	resources	impl	derived	GG2.GP3 GG2.GP8
G-M23	percentage of process tasks where responsibility and authority for performing them is not assigned	responsibilities	impl	derived	GG2.GP4 GG2.GP8
G-M24	percentage of staff who have been assessed to determine if training has been effective[11] commensurate with their job responsibilities (duplicated from OTA; effectiveness)	training	effectiveness	derived	GG2.GP5 GG2.GP8
G-M25	difference in planned versus actual designated work products that are subject to configuration control	controlled work products	impl	derived	GG2.GP6 GG2.GP8
G-M26	difference in planned versus actual stakeholders involved in the process	stakeholders	impl	derived	GG2.GP7 GG2.GP8
G-M27	percentage of processes whose performance against plan is measured	process performance	impl	derived	GG2.GP8 GG2.GP9
G-M28	difference in planned versus actual process performance	process performance	impl	derived	GG2.GP8 GG2.GP9
G-M29	percentage of significant deviations from the process plan without corrective actions	process performance; plan deviations	impl	derived	GG2.GP8 GG2.GP9
G-M30	percentage of significant deviations from the process plan with corrective actions that are on track per plan	process performance; plan deviations	impl	derived	GG2.GP8 GG2.GP9
G-M31	percentage of process problems (performance, execution) without corrective actions	process performance; process problems	impl	derived	GG2.GP8 GG2.GP9
G-M32	percentage of process problems with corrective actions that are on track per plan	process performance; process problems	impl	derived	GG2.GP8 GG2.GP9
G-M33	number of process risks referred to the risk management process	risk	impl	base of type count	GG2.GP8
G-M34	number of asset risks referred to the risk management process (applicable to ADM, EC, KIM, PM, TM)	risk	impl	base of type count	GG2.GP8
G-M35	number of process risks referred to the risk management process for which corrective action is pending (by risk rank) beyond threshold (schedule)	risk	impl	base of type count	GG2.GP8 GG2.GP10
G-M36	extent to which resilience[12] is improved as a result of taking action on CERT-RMM diagnostic results[13] as measured by, for example, a reduction in impact and consequences due to a disruptive event such as a security incident	resilience improvement	effectiveness	derived	GG2.GP8 GG2.GP9 GG2.GP10

[11] OTA:SG4.SP3 provides several approaches for assessing training effectiveness.

[12] This measure could apply to all 26 process areas, a selected set of process areas, or a targeted area of resilience improvement (such as selected specific goals and practices within the model scope for the diagnosis).

[13] Diagnostic results include the outcomes of CERT-RMM appraisals, Compass, or other forms of diagnosis. This measure could be stated as implementing CERT-RMM process areas, specific goals, and specific practices.

Asset Definition and Management (ADM)

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

Summary of Specific Goals and Practices

ADM:SG1 Establish Organizational Assets

ADM:SG1.SP1 Inventory Assets

ADM:SG1.SP2 Establish a Common Understanding

ADM:SG1.SP3 Establish Ownership and Custodianship

ADM:SG2 Establish the Relationship Between Assets and Services

ADM:SG2.SP1 Associate Assets with Services

ADM:SG2.SP2 Analyze Asset-Service Dependencies

ADM:SG3 Manage Assets

ADM:SG3.SP1 Identify Change Criteria

ADM:SG3.SP2 Maintain Changes to Assets and Inventory

Measures

ID[14]	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
ADM-M1	percentage of assets[15] that have been inventoried	asset inventory	impl	derived	ADM:SG1.SP1
ADM-M2	percentage of assets with/without a complete asset profile	asset inventory	impl	derived	ADM:SG1.SP2
ADM-M3	percentage of assets with/without a designated owner	asset inventory	impl	derived	ADM:SG1.SP3
ADM-M4	percentage of assets with/without a designated custodian (if applicable)	asset inventory	impl	derived	ADM:SG1.SP3
ADM-M5	percentage of assets that have designated owners but no custodians (if applicable)	asset inventory	impl	derived	ADM:SG1.SP3
ADM-M6	percentage of assets that have designated custodians but no owners	asset inventory	impl	derived	ADM:SG1.SP3
ADM-M7	percentage of assets that have been inventoried, by service	asset inventory	impl	derived	ADM:SG2.SP1
ADM-M8	percentage of assets that are not associated with one or more services	asset inventory	impl	derived	ADM:SG2.SP1
ADM-M9	elapsed time since the asset inventory was reviewed	asset inventory	impl	base of type schedule	ADM:SG1.SP1 ADM:SG3.SP1
ADM-M10	percentage of asset-service dependency conflicts with unimplemented or incomplete mitigation plans	asset-service dependencies	impl	derived	ADM:SG2.SP2

[14] The ID value is assigned based on the order in which the measure appears in CERT-RMM v1.1. Measures have been reordered here by the type of information.

[15] All references to assets and services in ADM and in all other PAs refer to high-value assets and high-value services. This qualifier applies throughout and is not included for ease of reading.

ID[14]	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
ADM-M11	percentage of asset-service dependency conflicts with no mitigation plans	asset-service dependen-cies	impl	derived	ADM:SG2.SP2
ADM-M12	number of discrepancies between the current inventory and the previous inventory	asset change management	impl	base of type count	ADM:SG3.SP1
ADM-M13	number of changes made to asset profiles in the asset inventory	asset change management	impl	base of type count	ADM:SG3.SP2
ADM-M14	number of changes to resilience require-ments as a result of asset changes	asset change management	impl	base of type count	ADM:SG3.SP2
ADM-M15	number of changes to service continuity plans as a result of asset changes	asset change management	impl	base of type count	ADM:SG3.SP2

Access Management (AM)

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

Summary of Specific Goals and Practices

AM:SG1 Manage and Control Access

AM:SG1.SP1 Enable Access

AM:SG1.SP2 Manage Changes to Access Privileges

AM:SG1.SP3 Periodically Review and Maintain Access Privileges

AM:SG1.SP4 Correct Inconsistencies

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
AM-M1	percentage of asset owners participating in establishing and maintaining access privileg-es for the assets that they own	access privileges	impl	derived	AM:SG1.SP1
AM-M2	percentage of access requests that adhere to the access control policy	access policy	impl	derived	AM:SG1.SP1
AM-M3	percentage of access acknowledgement forms that have been fully executed	access policy	impl	derived	AM:SG1.SP1
AM-M4	percentage of access requests denied (based on policy)	access requests	impl	derived	AM:SG1.SP1
AM-M5	percentage of approved access requests pending implementation beyond schedule	access requests	impl	derived	AM:SG1.SP1
AM-M6	number of duplicate access requests	access requests	impl	base of type count	AM:SG1.SP1
AM-M7	percentage of unapproved access requests that result in allowing access privileges (this should be zero)	access requests	effec-tiveness	derived	AM:SG1.SP1
AM-M8	percentage of access requests that do not reflect the requestor's role or job responsibili-ties (inadequate, excessive)	access requests	effec-tiveness	derived	AM:SG1.SP1

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
AM-M9	percentage of access privileges that are determined to be excessive or inappropriate based on the identity's role or job responsibilities	access privileges	effectiveness	derived	AM:SG1.SP3
AM-M10	elapsed time since access privileges were reviewed to ensure they reflect privileges assigned by the asset owner	access privileges	impl	base of type schedule	AM:SG1.SP3
AM-M11	rate of requests to change access privileges	access privileges	impl	derived	AM:SG1.SP2 AM:SG1.SP4
AM-M12	percentage of access privilege change requests approved/denied	access privileges	impl	derived	AM:SG1.SP2
AM-M13	percentage of corrective actions to address excessive or inappropriate levels of access privileges pending beyond schedule	access privileges	impl	derived	AM:SG1.SP4
AM-M14	elapsed time from a change in access privileges requiring deprovisioning to the actual deprovisioning (mean, median)	deprovisioning	effectiveness	derived	AM:SG1.SP4 ID:SG2.SP4
AM-M15	number of risks related to inappropriate or excessive levels of access privileges that have been referred to the risk management process	risk identification	impl	base of type count	AM:SG1.SP1 AM:SG1.SP4

Communications (COMM)

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

Summary of Specific Goals and Practices

COMM:SG1 Prepare for Resilience Communications

- COMM:SG1.SP1 Identify Relevant Stakeholders
- COMM:SG1.SP2 Identify Communications Requirements
- COMM:SG1.SP3 Establish Communications Guidelines and Standards

COMM:SG2 Prepare for Communications Management

- COMM:SG2.SP1 Establish a Resilience Communications Plan
- COMM:SG2.SP2 Establish a Resilience Communications Program
- COMM:SG2.SP3 Identify and Assign Plan Staff

COMM:SG3 Deliver Resilience Communications

- COMM:SG3.SP1 Identify Communications Methods and Channels
- COMM:SG3.SP2 Establish and Maintain Communications Infrastructure

COMM:SG4 Improve Communications

- COMM:SG4.SP1 Assess Communications Effectiveness
- COMM:SG4.SP2 Improve Communications

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
COMM-M1	confidence factor[16] that all stakeholders with a vested interest or vital role in resilience communications have been identified	communications stakeholders	impl	derived	COMM:SG1.SP1
COMM-M2	percentage of communications stakeholders for which roles have/have not been defined	communications stakeholders	impl	derived	COMM:SG1.SP1
COMM-M3	percentage of communications stakeholders for which stakeholder needs (types, frequencies, and levels of communication by specific circumstance) have/have not been defined	communications stakeholders	impl	derived	COMM:SG1.SP1
COMM-M4	percentage of communications stakeholders for which resilience communications and requirements have/have not been defined	communications stakeholders; communications requirements	impl	derived	COMM:SG1.SP2
COMM-M5	percentage of resilience communications requirements that cannot be met (by some meaningful categorization such as missing, inadequate, or untrained staff; missing or inadequate tools, techniques, methods, etc.— a.k.a. infrastructure)	communications requirements	impl	derived	COMM:SG1.SP2 COMM:SG2.SP3 COMM:SG3.SP2
COMM-M6	percentage of communications plan roles not covered in job descriptions	communications staff	impl	derived	COMM:SG2.SP3
COMM-M7	percentage of stakeholders (by type) for which communications methods and channels have/have not been identified	communications stakeholders; communications methods and channels	impl	derived	COMM:SG3.SP1
COMM-M8	number of new communications methods and channels	communications methods and channels	impl	base of type count	COMM:SG3.SP1
COMM-M9	percentage of methods and channels with sufficient infrastructure to support them	communications methods and channels	impl	derived	COMM:SG3.SP1
COMM-M10	number of communications delivered by event type, stakeholder type, method and channel type (or other meaningful categorization)	communications delivery	impl	base of type count	COMM:SG4.SP1
COMM-M11	percentage of communications methods and channels operating within expected tolerances (e.g., press release must be issued within one hour of a significant event)	communications delivery; communications methods and channels	effectiveness	derived	COMM:SG4.SP1
COMM-M12	change (increase or decrease) in length of time to commence communications by event type	communications delivery	impl	derived	COMM:SG4.SP1
COMM-M13	percentage of stakeholders that do not receive communications within expected tolerances, by stakeholder type and by event type	communications delivery; communications stakeholders	effectiveness	derived	COMM:SG4.SP1

[16] Refer to comparable measure and template in *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010], section 4.1.1.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
COMM-M14	number of communications methods and channels required to deliver the same or similar messages	communications delivery; communications methods and channels	impl	base of type count	COMM:SG4.SP1
COMM-M15	percentage of uptime or availability (downtime) of preferred communications methods, channels, and infrastructure	communications methods and channels; communications infrastructure	effectiveness	derived	COMM:SG4.SP1
COMM-M16	number of recommendations for improvement referred to the event, incident, service continuity, and crisis management processes	process improvement	impl	base of type count	COMM:SG4.SP1
COMM-M17	percentage of communications deficiencies and omissions for which corrective action is pending beyond schedule	communications deficiencies	effectiveness	derived	COMM:SG4.SP2
COMM-M18	number of service continuity plans that require updates as a result of communications deficiencies or omissions	communications deficiencies; service continuity plans	effectiveness	base of type count	COMM:SG4.SP2
COMM-M19	number of communications failures resulting from lack of adherence to resilience communications guidelines and standards	communications deficiencies; communications guidelines and standards	effectiveness	base of type count	COMM:SG1.SP3
COMM-M20	percentage of resilience communications objectives that are being achieved according to plan	plan status	impl	derived	COMM:SG2.SP1

Compliance (COMP)

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

Summary of Specific Goals and Practices

COMP:SG1 Prepare for Compliance Management

- COMP:SG1.SP1 Establish a Compliance Plan
- COMP:SG1.SP2 Establish a Compliance Program
- COMP:SG1.SP3 Establish Compliance Guidelines and Standards

COMP:SG2 Establish Compliance Obligations

- COMP:SG2.SP1 Identify Compliance Obligations
- COMP:SG2.SP2 Analyze Obligations
- COMP:SG2.SP3 Establish Ownership for Meeting Obligations

COMP:SG3 Demonstrate Satisfaction of Compliance Obligations

- COMP:SG3.SP1 Collect and Validate Compliance Data
- COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction

COMP:SG3.SP3 Remediate Areas of Non-Compliance

COMP:SG4 Monitor Compliance Activities

COMP:SG4.SP1 Evaluate Compliance Activities

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
COMP-M1	time expended to gather, organize, analyze, and report data for compliance obligations[17]	compliance data	impl	derived	COMP:SG2.SP1
COMP-M2	percentage of compliance obligation data collection activities that are/are not automated	compliance data	impl	derived	COMP:SG1.SP2 COMP:SG1.SP3
COMP-M3	number of compliance obligations (may require some prioritization of obligations such as high, medium, low)	obligation inventory	impl	base of type count	COMP:SG2.SP1
COMP-M4	percentage of compliance obligations that have been inventoried	obligation inventory	impl	derived	COMP:SG2.SP1
COMP-M5	percentage of compliance obligations with/without a designated owner (organizational unit, line of business)	obligation inventory	impl	derived	COMP:SG2.SP1 COMP:SG2.SP3
COMP-M6	number of external entities with agreements to meet compliance obligations	obligation inventory	impl	base of type count	COMP:SG1.SP3 COMP:SG2.SP1 EXD:SG1.SP1
COMP-M7	percentage of compliance obligations that rely upon external dependencies	obligation inventory	impl	derived	COMP:SG2.SP1 EXD:SG1.SP1
COMP-M8	percentage of compliance obligations that rely upon external entities	obligation inventory	impl	derived	COMP:SG2.SP1 EXD:SG1.SP1
COMP-M9	percentage of compliance obligations that are not met	obligation satisfaction	impl	derived	COMP:SG3.SP2
COMP-M10	percentage of compliance obligations not met by deadline	obligation satisfaction	impl	derived	COMP:SG3.SP2
COMP-M11	percentage of compliance activities that do not meet standards and guidelines	obligation satisfaction	impl	derived	COMP:SG3.SP2
COMP-M12	percentage of controls required solely to meet compliance obligations	obligation satisfaction	impl	derived	COMP:SG4.SP1
COMP-M13	percentage of service continuity guidelines and standards that are more/less stringent than required to meet compliance obligations	obligation satisfaction	impl	derived	SC:SG1.SP1 SC:SG1.SP2

[17] Any reference to "compliance obligations" includes "(by category, by source)" as part of the definition of the measure. It is omitted from measures for ease of reading.

COMP-M14	number of compliance risks (exceptions, non-compliance, remediation) referred to key stakeholders (the risk management process, the organization's governance process, etc.)	obligation remediation	impl; risk identifi-cation	base of type count	COMP:SG1. SP2 COMP:SG3. SP2 COMP:SG3. SP3
COMP-M15	percentage of compliance obligation violations requiring corrective action for which such action has not been taken as scheduled	obligation remediation	impl	derived	COMP:SG1. SP2
COMP-M16	percentage of compliance obligations that are conflicting (could also include duplicates, redundancies, and overlaps, but conflicts are likely of greatest interest)	obligation remediation	impl	derived	COMP:SG2. SP2 (COMP:SG1. SP2)
COMP-M17	percentage of compliance obligations requir-ing remediation for which the remediation action results in the obligation being met	obligation remediation	impl	derived	COMP:SG3. SP3
COMP-M18	cost to satisfy compliance obligations	cost of compliance	impl	base of type cost	COMP:SG4. SP1
COMP-M19	costs of non-compliance including: amount of fines and penalties levied for non-reporting amount of fines and penalties levied for non-compliance	cost of compliance	impl	base of type cost	COMP:SG3. SP2 COMP:SG2. SP1
COMP-M20	number of deficiencies in the compliance process that directly resulted in compliance obligations not being met	compliance process	effec-tiveness	base of type defect	COMP:SG4. SP1
COMP-M21	number of deficiencies in internal controls that directly resulted in compliance obligations not being met	compliance obligations; internal controls	effec-tiveness	base of type defect	COMP:SG4. SP1
COMP-M22	number of errors in the compliance process caused by inaccurate or unavailable data	compliance process; compliance data	effec-tiveness	base of type defect	COMP:SG3. SP1

Controls Management (CTRL)

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

Summary of Specific Goals and Practices

CTRL:SG1 Establish Control Objectives

CTRL:SG1.SP1 Define Control Objectives

CTRL:SG2 Establish Controls

CTRL:SG2.SP1 Define Controls

CTRL:SG3 Analyze Controls

CTRL:SG3.SP1 Analyze Controls

CTRL:SG4 Assess Control Effectiveness

CTRL:SG4.SP1 Assess Controls

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
CTRL-M1	confidence factor[18] that control objectives from all relevant management directives and guidelines have been identified at the enterprise level at the service level (perhaps by service type) at the asset level (perhaps by asset type)	control objectives	effectiveness	derived	CTRL:SG1.SP1
CTRL-M2	percentage of control objectives that have been prioritized (should be 100%)	control objectives	impl	derived	CTRL:SG1.SP1
CTRL-M3	percentage of enterprise-level controls for which responsibility has been confirmed or assigned[19]	enterprise controls	impl	derived	CTRL:SG2.SP1
CTRL-M4	percentage of enterprise-level controls that do not map to one or more control objectives	enterprise controls	impl	derived	CTRL:SG2.SP1
CTRL-M5	percentage of service-level controls for which responsibility has been confirmed or assigned	service controls	impl	derived	CTRL:SG2.SP1
CTRL-M6	percentage of service-level controls that do not map to one or more control objectives	service controls	impl	derived	CTRL:SG2.SP1
CTRL-M7	percentage of asset-level controls for which responsibility has been confirmed or assigned	asset controls	impl	derived	CTRL:SG2.SP1
CTRL-M8	percentage of asset-level controls that do not map to one or more control objectives	asset controls	impl	derived	CTRL:SG2.SP1
CTRL-M9	percentage of control objectives that are fully satisfied by existing controls at the enterprise level at the service level (perhaps by service type) at the asset level (perhaps by asset type)	control objective satisfaction	Impl	derived	CTRL:SG3.SP1[20]
CTRL-M10	percentage of controls that satisfy multiple control objectives (and mean, median number of control objectives satisfied)	control objective satisfaction	Impl	derived	CTRL:SG3.SP1
CTRL-M11	percentage of controls that require updates to address gaps[21] (perhaps by control objective)	control objective satisfaction; control gaps	Impl	derived	CTRL:SG3.SP1
CTRL-M12	percentage of control objectives that are affected by updated controls	control objective satisfaction; control changes	Impl	derived	CTRL:SG3.SP1

[18] Refer to comparable measure and template in *Measuring Operational Resilience Using the CERT Resilience Management Model* [Allen 2010], section 4.1.1.

[19] Confirmation applies to existing and updated controls; assignment is required for new controls.

[20] CTRL:SG3 establishes a baseline analysis of the extent to which existing controls and proposed new controls cover and achieve control objectives for the resilience of services and supporting assets. CTRL:SG4 uses this established baseline as the foundation for periodically assessing the extent to which controls continue to achieve control objectives and the extent to which control objectives continue to meet resilience requirements.

[21] Where control objectives are not adequately satisfied by existing controls

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
CTRL-M13	number of proposed new controls that are required to address gaps (perhaps by control objective)	control objective satisfaction; control gaps	Impl	base of type count	CTRL:SG3.SP1
CTRL-M14	percentage of control objectives that are affected by proposed new controls	control objective satisfaction; control changes	Impl	derived	CTRL:SG3.SP1
CTRL-M15	percentage of controls that are redundant	control redundancy	Impl	derived	CTRL:SG3.SP1
CTRL-M16	percentage of control objectives that are affected by redundant controls	control objectives; control redundancy	Impl	derived	CTRL:SG3.SP1
CTRL-M17	percentage of controls that are conflicting (enterprise, service, asset)	control conflicts	Impl	derived	CTRL:SG3.SP1
CTRL-M18	percentage of control objectives that are affected by conflicting controls	control objectives; control conflicts	Impl	derived	CTRL:SG3.SP1
CTRL-M19	percentage of control issues that are resolved in the required timeframe: gaps resulting from unsatisfied control objectives redundant controls conflicting controls	control issues; control changes	impl	derived	CTRL:SG3.SP1
CTRL-M20	for issues that are not resolved, number of new/updated risks[22] (by risk rank) resulting from unsatisfied control objectives unaddressed redundant controls unaddressed conflicting controls	control issues; risk identification	impl	base of type count	CTRL:SG3.SP1
CTRL-M21	time and resources expended to conduct an analysis of controls (establish the baseline)	controls analysis	impl	derived	CTRL:SG3.SP1
CTRL-M22	time and resources expended to conduct an assessment of controls (periodic)	controls assessment	impl	derived	CTRL:SG4.SP1
CTRL-M23	number of problem areas resulting from the assessment of controls (perhaps by control objective)	controls assessment	impl	base of type count	CTRL:SG4.SP1
CTRL-M24	number of problem areas escalated to higher level managers for review	controls assessment; control issues	impl	base of type count	CTRL:SG4.SP1
CTRL-M25	percentage of control objectives requiring remediation plans	control objectives	impl	derived	CTRL:SG4.SP1
CTRL-M26	for controls that can be automated, percentage of controls that have been fully automated	control automation	impl	derived	CTRL:SG4.SP1

[22] Risks result where the priority of a control objective and any resulting control gaps do not warrant further investment in updated or new controls.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
CTRL-M27	percentage of problem areas[23] that are/are not resolved within threshold (as scheduled): gaps resulting from unsatisfied control objectives redundant controls conflicting controls	control issues; control changes	impl	derived	CTRL:SG4.SP1
CTRL-M28	percentage reduction in number of controls	control changes	impl; possibly effectiveness	derived	CTRL:SG4.SP1
CTRL-M29	number of risks resulting from unresolved problems in the internal control system that are referred to the risk management process	control issues; risk identification	impl	base of type count	CTRL:SG4.SP1
CTRL-M30	number of updates to service continuity plans that result from changes to the internal control system	service continuity plans; control changes	impl	base of type count	CTRL:SG4.SP1

Environmental Control (EC)

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

Summary of Specific Goals and Practices

EC:SG1 Establish and Prioritize Facility Assets

EC:SG1.SP1 Prioritize Facility Assets

EC:SG1.SP2 Establish Resilience-Focused Facility Assets

EC:SG2 Protect Facility Assets

EC:SG2.SP1 Assign Resilience Requirements to Facility Assets

EC:SG2.SP2 Establish and Implement Controls

EC:SG3 Manage Facility Asset Risk

EC:SG3.SP1 Identify and Assess Facility Asset Risk

EC:SG3.SP2 Mitigate Facility Risks

EC:SG4 Control Operational Environment

EC:SG4.SP1 Perform Facility Sustainability Planning

EC:SG4.SP2 Maintain Environmental Conditions

EC:SG4.SP3 Manage Dependencies on Public Services

EC:SG4.SP4 Manage Dependencies on Public Infrastructure

EC:SG4.SP5 Plan for Facility Retirement

[23] May want to limit this measure to those problem areas that require remediation plans.

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EC-M1	percentage of facility assets that have been inventoried	asset inventory	impl	derived	ADM:SG1.SP1
EC-M2	percentage of facility assets with/without a complete asset profile (such as no stated resilience requirements)	asset inventory	impl	derived	ADM:SG1.SP2 EC:SG2.SP1
EC-M3	percentage of facility assets with/without a designated owner	asset inventory	impl	derived	ADM:SG1.SP3
EC-M4	percentage of facility assets with/without a designated custodian (if applicable)	asset inventory	impl	derived	ADM:SG1.SP3
EC-M5	percentage of facility assets that have designated owners but no custodians (if applicable)	asset inventory	impl	derived	ADM:SG1.SP3
EC-M6	percentage of facility assets that have designated custodians but no owners	asset inventory	impl	derived	ADM:SG1.SP3
EC-M7	percentage of facility assets that have been inventoried, by service (if applicable)	asset inventory	impl	derived	ADM:SG2.SP1
EC-M8	percentage of facility assets that are not associated with one or more services (if applicable)	asset inventory	impl	derived	ADM:SG2.SP1
EC-M9	elapsed time since the facility asset inventory was reviewed	asset inventory	impl	base of type schedule	ADM:SG1.SP1 ADM:SG3.SP1
EC-M10	percentage of facility asset-service dependency conflicts with unimplemented or incomplete mitigation plans	asset-service dependencies	impl	derived	ADM:SG2.SP2
EC-M11	percentage of facility asset-service dependency conflicts with no mitigation plans	asset-service dependencies	impl	derived	ADM:SG2.SP2
EC-M12	number of discrepancies between the current inventory and the previous inventory	asset inventory	impl	base of type count	ADM:SG3.SP1
EC-M13	number of changes made to asset profiles in the facility asset inventory	asset inventory	impl	base of type count	ADM:SG3.SP2
EC-M14	number of changes to resilience requirements as a result of facility asset changes	asset change management	impl	base of type count	ADM:SG3.SP2
EC-M15	number of changes to service continuity plans as a result of facility asset changes	asset change management	impl	base of type count	ADM:SG3.SP2
EC-M16	percentage of facility assets that are designated as high-value assets	asset inventory	impl	derived	EC:SG1.SP1
EC-M17	elapsed time since review and validation of high-value facility assets and their priorities	asset inventory	impl	derived	EC:SG1.SP1
EC-M18	percentage of facility assets that are resilience-focused (those required for service continuity & service restoration)	asset inventory	impl	derived	EC:SG1.SP2
EC-M19	elapsed time since review and reconciliation of resilience-focused facility assets	asset inventory	impl	derived	EC:SG1.SP2
EC-M20	percentage of facility assets without assigned/defined resilience requirements	asset requirements	impl	derived	EC:SG2.SP1

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EC-M21	percentage of facility assets with assigned/defined resilience requirements that are undocumented	asset requirements	impl	derived	EC:SG2.SP1
EC-M22	percentage of facility assets that do not satisfy their resilience requirements	asset requirement	impl	derived	EC:SG2.SP1
EC-M23	percentage of facility assets with no or missing protection controls	asset controls	impl; possibly effectiveness	derived	EC:SG2.SP2
EC-M24	percentage of facility assets with no or missing sustainment controls (including controls over design, construction, and leasing)	asset controls	impl; possibly effectiveness	derived	EC:SG2.SP2
EC-M25	percentage of facility asset controls (protection and sustainment) that are ineffective or inadequate as demonstrated by: unsatisfied control objectives unmet resilience requirements outstanding control assessment problem areas above established thresholds and without remediation plans	asset controls	impl; possibly effectiveness	derived	EC:SG2.SP2
EC-M26	percentage of facility asset control deficiencies not resolved by scheduled due date (refer to CTRL measures for categories of control deficiencies)	asset controls	impl	derived	EC:SG2.SP2
EC-M27	elapsed time since review of the effectiveness of facility asset controls	asset controls	impl	base of type schedule	EC:SG2.SP2
EC-M28	elapsed time since risk assessment of facility assets performed	asset risk	impl	base of type schedule	EC:SG3.SP1
EC-M29	percentage of facility assets for which business impact valuation[24] has not been performed	asset risk	impl	derived	EC:SG3.SP1
EC-M30	percentage of facility assets for which a risk assessment has not been performed and documented (per policy or other guidelines) and according to plan	asset risk	impl	derived	EC:SG3.SP1
EC-M31	percentage of facility asset risks that have not been assigned to a responsible party for action, tracking, and closure	asset risk	impl	derived	EC:SG3.SP2
EC-M32	percentage of facility asset risks[25] with a disposition of “mitigate or control” that do not have a defined mitigation plan	asset risk	impl	derived	EC:SG3.SP2 [26]
EC-M33	percentage of facility asset risks with a “mitigate or control” disposition that are not effectively mitigated by their mitigation plans	asset risk	effectiveness	derived	EC:SG3.SP2

[24] Business impact valuation can be either qualitative (high, medium, low) or quantitative (based on levels of loss or damage, fines, number of customers lost, disruption in access, etc.).

[25] This measure also appears in RISK M4-1. For ease of use of an individual PA (vs. ease of maintenance and consistency), we have decided to replicate some (but not all) risk-related measures in the individual asset PAs that are identified generally in the list of RISK PA measures.

[26] SG3.SP2 subpractice 7 states, “Collect performance measures on the risk management process.” No such measures are included here in EC; refer to the RISK PA.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EC-M34	percentage of realized risks for facility assets that exceed established risk parameters	asset risk	effectiveness	derived	EC:SG3.SP2
EC-M35	percentage of facility assets for which a business impact analysis has been performed	asset continuity	impl	derived	EC:SG4.SP1
EC-M36	elapsed time since business impact analysis of facility assets performed	asset risk	impl	base of type schedule	EC:SG3.SP1 EC:SG4.SP1
EC-M37	percentage of facilities with service continuity plans	asset continuity	impl	derived	EC:SG4.SP1
EC-M38	percentage of facilities that are included as associated assets by service-based continuity plans	asset continuity	impl	derived	EC:SG4.SP1
EC-M39	percentage of external entities that are not meeting service level agreements for maintaining facility assets	asset maintenance	impl	derived	EC:SG4.SP2
EC-M40	percentage of facility assets that are not maintained at required maintenance levels (service intervals, specifications, etc.)	asset maintenance	impl	derived	EC:SG4.SP2
EC-M41	percentage of facility maintenance activities that are not completed as scheduled	asset maintenance	impl	derived	EC:SG4.SP2
EC-M42	elapsed time since facility maintenance performed	asset maintenance	impl	base of type schedule	EC:SG4.SP2
EC-M43	downtime statistics for process control systems, for example: physical access systems such as card readers physical access monitoring such as surveillance cameras support systems such as HVAC and fire suppression	asset maintenance	impl	derived	EC:SG4.SP2
EC-M44	percentage of facilities with dependencies on public services that are documented in service continuity plans or other appropriate form	asset dependencies	impl	derived	EC:SG4.SP3
EC-M45	percentage of facilities with dependencies on public infrastructure that are documented in service continuity plans or other appropriate form	asset dependencies	impl	derived	EC:SG4.SP4
EC-M46	percentage of facilities to be retired with a plan for facility retirement or, alternatively, a service continuity plan that addresses facility retirement	asset retirement	impl	derived	EC:SG4.SP5
EC-M47	percentage of facilities planned for retirement that are not retired according to plan	asset retirement	impl	derived	EC:SG4.SP5
EC-M48	number of violations of access control policies for facility assets	policy	impl	base of type count	EC:GG2.GP 1
EC-M49	percentage of intrusions into facility assets where impact exceeds threshold	asset intrusions	impl	derived	none (IMC-related)
EC-M50	percentage of clean desk and screen policies that are met (no violations, all exceptions approved)	policy	impl	derived	EC:GG2.GP 1

Enterprise Focus (EF)

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

Summary of Specific Goals and Practices

EF:SG1 Establish Strategic Objectives

EF:SG1.SP1 Establish Strategic Objectives

EF:SG1.SP2 Establish Critical Success Factors

EF:SG1.SP3 Establish Organizational Services

EF:SG2 Plan for Operational Resilience

EF:SG2.SP1 Establish an Operational Resilience Management Plan

EF:SG2.SP2 Establish an Operational Resilience Management Program

EF:SG3 Establish Sponsorship

EF:SG3.SP1 Commit Funding for Operational Resilience Management

EF:SG3.SP2 Promote a Resilience-Aware Culture

EF:SG3.SP3 Sponsor Resilience Standards and Policies

EF:SG4 Provide Resilience Oversight

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

EF:SG4.SP2 Perform Resilience Oversight

EF:SG4.SP3 Establish Corrective Actions

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EF-M1	percentage of critical success factors that are attainable per their key performance indicators	CSF status	impl	derived	EF:SG1.SP2
EF-M2	percentage of services for which a complete service profile has been documented in the service repository	services	impl	derived	EF:SG1.SP3
EF-M3	percentage of services determined to be high-value	services	impl	derived	EF:SG1.SP3
EF-M4	percentage of service profiles and service levels that have been reviewed within their review time frame	services	impl	derived	EF:SG1.SP3
EF-M5	percentage of resilience objectives that are being achieved according to plan	plan status	impl	derived	EF:SG2.SP1
EF-M6	percentage of operational resilience management plan commitments that are being met according to plan	plan status	impl	derived	EF:SG2.SP1
EF-M7	percentage of operational resilience management program and process activities for which adequate funds have been allocated	resources (funding)	impl	derived	EF:SG2.SP2 EF:SG3.SP1
EF-M8	percentage of operational resilience management program and process activities for which adequate staff have been allocated	resources (staff)	impl	derived	EF:SG2.SP2

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EF-M9	percentage of staff demonstrating resilience awareness commensurate with job descriptions, as measured by the presence of stated resilience performance goals and objectives and regular review of these for satisfaction or correction	cultural awareness	impl	derived	EF:SG3.SP2
EF-M10	percentage of external entity relationships for which resilience requirements have been specified in the agreements with these entities (see also EXD)	cultural awareness; candidate key indicator	impl	derived	EF:SG3.SP2 EF:SG4.SP2
EF-M11	percentage of external entity relationships for which resilience requirements have been implemented per the agreements with these entities (see also EXD)	cultural awareness; candidate key indicator	impl	derived	EF:SG3.SP2 EF:SG4.SP2
EF-M12	percentage of higher-level managers with explicit resilience goals	sponsorship	impl	derived	EF:SG3.SP2
EF-M13	percentage of higher-level managers who are promoting and communicating resilience as measured by satisfactory performance evaluations	sponsorship	impl	derived	EF:SG3.SP2
EF-M14	percentage of acculturation of resilience awareness that is the direct result of sponsorship (by staff group, by organizational unit)	sponsorship	impl	derived	EF:SG3.SP2
EF-M15	percentage of higher-level managers that are fulfilling their commitments to manage resilience per policy as measured by satisfactory performance evaluations	sponsorship	impl	derived	EF:SG3.SP3 EF:SG4.SP1
EF-M16	percentage of committee charters that include resilience responsibilities	oversight	impl	derived	EF:SG4.SP1
EF-M17	percentage of key operational resilience management roles for which responsibilities, accountabilities, and authority are assigned and required skills identified, including key governance stakeholders	oversight	impl	derived	EF:SG4.SP1
EF-M18	percentage of board meetings and/or designated committee meetings for which operational resilience management is on the agenda	oversight	impl	derived	EF:SG4.SP1
EF-M19	percentage of key indicators (KPIs, KRIs, KCIs) that are within acceptable ranges	oversight	impl	derived	EF:SG4.SP2
EF-M20	percentage of key indicators that are outside of acceptable ranges and for which a corrective action plan exists	oversight	impl	derived	EF:SG4.SP2 EF:SG4.SP3
EF-M21	percentage of key indicators with corrective action plans where actions taken were successful in bringing indicators within acceptable ranges	oversight	impl	derived	EF:SG4.SP3
EF-M22	elapsed calendar time since key indicators were reported to governance stakeholders	oversight	impl	base of type schedule	EF:SG4.SP2
EF-M23	percentage of required internal and external audits completed and reviewed by the board or other designated oversight body	oversight	impl	derived	EF:SG4.SP2
EF-M24	percentage of audit findings that have been resolved	oversight	impl	derived	EF:SG4.SP2

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EF-M25	percentage of incidents that caused damage, compromise, or loss beyond established thresholds to the organization's assets and services (categorized by asset, by service, by incident type, etc.)	candidate key indicator	impl	derived	EF:SG4.SP2
EF-M26	dollar amount of estimated damage or loss resulting from all incidents (categorized by asset, by service, by incident type, etc.)	candidate key indicator	impl	base of type cost	EF:SG4.SP2
EF-M27	percentage of organizational units with established service continuity plan(s) for the services that require such a plan where the unit is the designated owner	candidate key indicator	impl	derived	EF:SG4.SP2 SC:SG3.SP1
EF-M28	percentage of key external resilience requirements (laws, regulations, standards, etc.) for which the organization has been deemed by objective audit to be in compliance (see also COMP)	candidate key indicator	impl	derived	EF:SG4.SP2
EF-M29	level of capability achieved in other operational resilience management process areas	candidate key indicator	impl	base of type ordinal/ratio	EF:SG4.SP2
EF-M30	percentage of operational resilience management policies that are met	candidate key indicator	impl	derived	EF:SG4.SP2
EF-M31	number of policy violations for policies related to each operational resilience management process area	candidate key indicator	impl	base of type count	EF:SG4.SP2
EF-M32	percentage of high-value assets (by asset type) for which a comprehensive strategy and internal control system have been implemented to mitigate risks as necessary and to maintain these risks within acceptable thresholds	candidate key indicator	impl	derived	EF:SG4.SP2
EF-M33	number of enterprise-level risks referred to the risk management process	risk identification	impl	base of type count	EF:SG4.SP2
EF-M34	percentage of CERT-RMM practices (based on a specific model scope) that are addressed by governance (EF) activities	governance scope	impl; possibly effectiveness	derived	none

External Dependencies Management (EXD)

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

Summary of Specific Goals and Practices

EXD:SG1 Identify and Prioritize External Dependencies

EXD:SG1.SP1 Identify External Dependencies

EXD:SG1.SP2 Prioritize External Dependencies

EXD:SG2 Manage Risks Due to External Dependencies

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

EXD:SG2.SP2 Mitigate Risks Due to External Dependencies

EXD:SG3 Establish Formal Relationships

EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies

EXD:SG3.SP2 Establish Resilience Specifications for External Dependencies

EXD:SG3.SP3 Evaluate and Select External Entities

EXD:SG3.SP4 Formalize Relationships

EXD:SG4 Manage External Entity Performance

EXD:SG4.SP1 Monitor External Entity Performance

EXD:SG4.SP2 Correct External Entity Performance

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EXD-M1	by external dependency, in priority order: percentage of services that rely on the external dependency percentage of assets that rely on the external dependency	definition of external dependencies	impl	derived	EXD:SG1.SP1 EXD:SG1.SP2
EXD-M2	by external entity, in priority order: number of services that rely on[27] the external entity, by type of service (if applicable) number of assets that rely on the external entity, by type of asset number of external dependencies which rely on the external entity[28] number of compliance obligations that rely on or apply to the external entity monetary value of the relationship with the external entity number of agreement changes by change type number of entities external to itself upon which the external entity relies to meet its obligations	identification of external entities	impl	base of type count	EXD:SG1.SP1 EXD:SG1.SP2[29]
EXD-M3	percentage of assets that rely on external entities	identification of external entities	impl	derived	EXD:SG1.SP1 EXD:SG1.SP2
EXD-M4	percentage of services that rely on external entities	identification of external entities	impl	derived	EXD:SG1.SP1 EXD:SG1.SP2

[27] "Rely on" includes accessed, owned, responsible for, developed, controlled, used, operated, or otherwise influenced by the external entity.

[28] This should be supported by some type of visual traceability mapping that shows the relationships between external entities and external dependencies.

[29] Prioritization of external entities not explicitly addressed in SG1.SP2 but can be inferred

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EXD-M5	number of external entities by relationship status (RFP, source selection, awarded, agreement/contract executed, performing as expected, out of compliance, in dispute or litigation, terminated, renewed, etc.)	identification of external entities	impl	base of type count	EXD:SG1.SP1 EXD:SG3.SP4 EXD:SG4.SP1 EXD:SG4.SP2
EXD-M6	number of external entities at each CERT-RMM capability level by process area[30]	definition of external entities	impl	base of type count	none
EXD-M7	percentage of external dependencies without a designated owner	definition of external dependencies	impl	derived	EXD:SG1.SP1
EXD-M8	percentage of external entities without a designated owner	identification of external entities	impl	derived	EXD:SG1.SP1
EXD-M9	percentage of external dependencies involved in meeting compliance obligations	definition of external dependencies	impl	derived	EXD:SG1.SP1
EXD-M10	percentage of external entities involved in meeting compliance obligations	identification of external entities	impl	derived	EXD:SG1.SP1
EXD-M11	number of external entities that are providing “commodity” services (easily replaced)	identification of external entities	impl	base of type count	EXD:SG1.SP1
EXD-M12	number of external entities that are providing “specialized” services (difficult to replace)	identification of external entities	impl	base of type count	EXD:SG1.SP1
EXD-M13	number of external entities in the same geographic region (for assessing geographic and socio-political risk)	identification of external entities	impl	base of type count	EXD:SG1.SP1
EXD-M14	number of external entities for which the relationship is managed by another part of the organization than the one owning the relationship	identification of external entities	impl	base of type count	EXD:SG1.SP1
EXD-M15	percentage of external dependencies that have not been reviewed and updated as scheduled	update of external dependencies	impl	derived	EXD:SG1.SP1 EXD:SG3.SP1 EXD:SG3.SP2
EXD-M16	elapsed time since risk assessment of external dependencies	external dependency risk	impl	base of type schedule	EXD:SG2.SP1
EXD-M17	percentage of external dependencies for which a risk assessment has not been performed and documented (per policy or other guidelines) according to plan	external dependency risk	impl	derived	EXD:SG2.SP1
EXD-M18	percentage of external dependency risks that have not been assigned to a responsible party for action, tracking, and closure	external dependency risk	impl	derived	EXD:SG2.SP2

[30] A CERT-RMM class A appraisal is required to assign a capability level. All external entities may not have performed such an appraisal.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EXD-M19	percentage of external dependency risks[31] with a disposition of "mitigate or control" that do not have a defined mitigation plan	external dependency risk	impl	derived	EXD:SG2.SP2
EXD-M20	percentage of external dependency risks with a "mitigate or control" disposition that are not effectively mitigated by their mitigation plans	external dependency risk	impl	derived	EXD:SG2.SP2
EXD-M21	percentage of realized risks for external dependencies that exceed established risk parameters	external dependency risk	effectiveness	derived	EXD:SG2.SP2
EXD-M22	percentage of RFPs for external entities that do not include resilience specifications	external entity selection	impl	derived	EXD:SG3.SP3
EXD-M23	percentage of candidate external entities whose due diligence process is on track per plan	external entity selection	impl	derived	EXD:SG3.SP3
EXD-M24	percentage of selected external entities without documented selection and decision rationale (this should be zero)	external entity selection	impl	derived	EXD:SG3.SP3
EXD-M25	number of resilience specifications unmet by the selected external entity	external entity selection	impl	base of type count	EXD:SG3.SP3
EXD-M26	number of resilience specifications unmet by the selected external entity that are identified as risks to be managed (ranked)	external entity selection	impl	base of type count	EXD:SG3.SP3
EXD-M27	percentage of agreements/contracts with external entities with specifications that have been waived as a result of negotiations	external entity agreements	impl	derived	EXD:SG3.SP4
EXD-M28	percentage of external entities that are achieving all specifications as defined in the agreement	external entity agreements	impl	derived	EXD:SG4.SP1
EXD-M29	percentage of external entity agreements that have not been reviewed as scheduled (including in response to changes in enterprise and resilience specifications)	external entity status	impl	derived	EXD:SG3.SP1 EXD:SG2.SP2
EXD-M30	percentage of external entities whose status (monitoring and inspection activities) has not been reviewed as scheduled	external entity status	impl	derived	EXD:SG4.SP1
EXD-M31	percentage of external entities that have undergone, as required by agreement/contract: • reviews • risk assessments • testing, evaluations • inspections • audits	external entity status	impl	derived	EXD:SG4.SP1
EXD-M32	percentage of external entities with corrective actions that have not been implemented as scheduled	external entity status	impl	derived	EXD:SG4.SP2
EXD-M33	percentage of external entities whose deliverables have failed to pass inspection	external entity status	impl	derived	EXD:SG4.SP1

[31] This measure also appears in RISK M4-1. For ease of use of an individual PA (vs. ease of maintenance and consistency), we have decided to replicate some (but not all) risk-related measures in the individual asset PAs that are identified generally in the list of RISK PA measures.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
EXD-M34	for all or specific external entities, elapsed time since last: • risk assessment • performance review • compliance audit • joint service continuity exercise	external entity status; external entity risk	impl	base of type schedule	EXD:SG4.SP1
EXD-M35	for all applicable external entities, elapsed time since source code was last updated in source code escrow	external entity status	impl	base of type schedule	EXD:SG4.SP1
EXD-M36	percentage of external entity risks that have not been assigned to a responsible party for action, tracking, and closure	external entity risk	impl	derived	EXD:SG4.SP1
EXD-M37	percentage of realized risks for external entities that exceed established risk parameters	external entity risk	effectiveness	derived	EXD:SG4.SP1
EXD-M38	percentage of external entities whose financial health is at risk (beyond risk parameters)	external entity risk	impl	derived	EXD:SG4ssssss.SP1
EXD-M39	percentage of external entities whose performance deviates sufficiently from specifications (beyond risk parameters) to cause a risk to be referred to the risk management process	external entity risk	impl	derived	EXD:SG4.SP1
EXD-M40	percentage of external entities that play a key role in fulfilling service continuity plans during disruptive events	external entity service continuity	impl	derived	none
EXD-M41	percentage of external entities that have tested their service continuity plans, including participating in tests conducted of organization's service continuity plans	external entity service continuity	impl	derived	none
EXD-M42	percentage of external entities that failed to perform as expected during a disruptive event	external entity service continuity	impl	derived	none

Financial Resource Management (FRM)

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

Summary of Specific Goals and Practices

FRM:SG1 Establish Financial Commitment

FRM:SG1.SP1 Commit Funding for Operational Resilience Management

FRM:SG1.SP2 Establish Structure to Support Financial Management

FRM:SG2 Perform Financial Planning

FRM:SG2.SP1 Define Funding Needs

FRM:SG2.SP2 Establish Resilience Budgets

FRM:SG2.SP3 Resolve Funding Gaps

FRM:SG3 Fund Resilience Activities

FRM:SG3.SP1 Fund Resilience Activities

FRM:SG4 Account for Resilience Activities

FRM:SG4.SP1 Track and Document Costs

FRM:SG4.SP2 Perform Cost and Performance Analysis

FRM:SG5 Optimize Resilience Expenditures and Investments

FRM:SG5.SP1 Optimize Resilience Expenditures

FRM:SG5.SP2 Determine Return on Resilience Investments

FRM:SG5.SP3 Identify Cost Recovery Opportunities

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
FRM-M1	elapsed time since the business case for the operational resilience management (ORM) system was reviewed and updated	resilience business case	impl	base of type schedule	FRM:SG1.SP1
FRM-M2	elapsed time since ORM system funding was reviewed	resilience funding	impl	base of type schedule	FRM:SG1.SP1
FRM-M3	elapsed time since ORM system funding was reviewed as part of the organization's strategic plan budgeting exercise	resilience funding	impl	base of type schedule	FRM:SG1.SP1
FRM-M4	difference in planned versus actual funding for the ORM system	resilience funding	impl; possibly effectiveness	derived	FRM:SG1.SP1
FRM-M5	elapsed time since responsibility and accountability for resilience budgeting, funding, and accounting activities were reviewed	resilience financial structure	impl	base of type schedule	FRM:SG1.SP2
FRM-M6	percentage of resilience activities for which historical financial cost data is used as the basis for developing funding requirements	resilience funding	impl	derived	FRM:SG2.SP1
FRM-M7	percentage of resilience funding assumptions that have been validated by comparison to resilience requirements	resilience funding	impl	derived	FRM:SG2.SP1
FRM-M8	cost of resilience (COR) calculations	resilience cost	impl	derived	FRM:SG4.SP1 FRM:SG4.SP2 FRM:SG5.SP2
FRM-M9	return on resilience investment (RORI) calculations	resilience cost; resilience benefit	impl	derived	FRM:SG4.SP1 FRM:SG4.SP2 FRM:SG5.SP2
FRM-M10	percentage of resilience costs that are included as part of standard costs for services and products (chargebacks)	resilience cost	impl	derived	FRM:SG5.SP3
FRM-M11	percentage of assets and services for which optimization[32] calculations have been performed	resilience cost; resilience benefit	impl	derived	FRM:SG5.SP1
FRM-M12	percentage of optimization opportunities for which no action has been taken	resilience cost; resilience benefit	impl	derived	FRM:SG5.SP1 FRM:SG5.SP2
FRM-M13	percentage of resilience activities with required budgets assigned, allocated, and applied, organized by organizational unit, project, asset, and service or other meaningful categorization scheme	resilience budgeting	impl	derived	FRM:SG2.SP2
FRM-M14	elapsed time since resilience budgets were reviewed and updated	resilience budgeting	impl	base of type schedule	FRM:SG2.SP2 FRM:SG4.SP1

[32] The costs of attaining and sustaining an adequate level of operational resilience for an asset or service must be optimized against the value of the asset or service in order to rationalize and maximize the organization's investment in resilience.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
FRM-M15	elapsed time since resilience budgets were reviewed to confirm their adequacy to meet resilience performance measures	resilience budgeting	impl	base of type schedule	FRM:SG2.SP2
FRM-M16	percentage of resilience activities subject to off-cycle or off-budget funding requests	resilience budgeting	effective-ness	derived	FRM:SG3.SP1
FRM-M17	percentage of resilience activities tracking to planned budgets	resilience budgeting	effective-ness	derived	FRM:SG3.SP1
FRM-M18	difference in planned versus actual cost for the ORM system	resilience cost	effective-ness	derived	FRM:SG4.SP1
FRM-M19	percentage of resilience activities with budget variances outside of established thresholds for which resolution plans have been developed to reduce or eliminate these variances	resilience budgeting	impl	derived	FRM:SG4.SP1 FRM:SG4.SP2
FRM-M20	percentage of financial exceptions re-ported to oversight managers and commit-tees	resilience budgeting	impl	derived	FRM:SG4.SP2
FRM-M21	percentage of resilience activities without required budget allocations for which gap and risk analysis has been performed	resilience budgeting; risk identifi-cation	impl	derived	FRM:SG2.SP3
FRM-M22	number of budget shorfall risks referred to the risk management process	risk identifi-cation	impl	base of type count	FRM:SG2.SP3

Human Resource Management (HRM)

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

Summary of Specific Goals and Practices

HRM:SG1 Establish Resource Needs

- HRM:SG1.SP1 Establish Baseline Competencies
- HRM:SG1.SP2 Inventory Skills and Identify Gaps
- HRM:SG1.SP3 Address Skill Deficiencies

HRM:SG2 Manage Staff Acquisition

- HRM:SG2.SP1 Verify Suitability of Candidate Staff
- HRM:SG2.SP2 Establish Terms and Conditions of Employment

HRM:SG3 Manage Staff Performance

- HRM:SG3.SP1 Establish Resilience as a Job Responsibility
- HRM:SG3.SP2 Establish Resilience Performance Goals and Objectives
- HRM:SG3.SP3 Measure and Assess Performance
- HRM:SG3.SP4 Establish Disciplinary Process

HRM:SG4 Manage Changes to Employment Status

- HRM:SG4.SP1 Manage Impact of Position Changes

HRM:SG4.SP2 Manage Access to Assets

HRM:SG4.SP3 Manage Involuntary Terminations

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
HRM-M1	percentage of job descriptions in which resilience competencies and skills are identified	resilience skill needs	impl	derived	HRM:SG1.SP1
HRM-M2	percentage of job descriptions with documented terms and conditions	job descriptions	impl	derived	HRM:SG2.SP2
HRM-M3	percentage of job descriptions with documented resilience obligations	job descriptions	impl	derived	HRM:SG2.SP2HRM:SG3.SP1
HRM-M4	percentage of vital staff with resilience skill deficiencies	resilience skill needs	impl	derived	HRM:SG1.SP2
HRM-M5	cost required to address resilience skill gaps	resilience skill needs; resilience cost	impl	base of type cost	HRM:SG1.SP3
HRM-M6	schedule required to address resilience skill gaps	resilience skill needs	impl	base of type schedule	HRM:SG1.SP3
HRM-M7	effort required to address resilience skill gaps	resilience skill needs	impl	base of type effort	HRM:SG1.SP3
HRM-M8	percentage of resilience training delivered as scheduled	resilience skill needs; resilience training	impl	derived	HRM:SG1.SP3
HRM-M9	rate of changes to the resilience skills inventory	skills inventory	impl	derived	HRM:SG1.SP2
HRM-M10	elapsed time since the resilience skills inventory was compared to baseline resilience competencies and skills	skills inventory	impl	base of type schedule	HRM:SG1.SP2
HRM-M11	percentage of acquired vital staff that have met pre-employment verification criteria (baseline and job-specific)	staff suitability	impl	derived	HRM:SG2.SP1
HRM-M12	percentage of acquired staff that have signed agreements to acknowledge and consent to employment terms and conditions	terms and conditions of employment	impl	derived	HRM:SG2.SP2
HRM-M13	percentage of confidentiality and non-compete agreements executed for people in sensitive positions	terms and conditions of employment	impl	derived	HRM:SG2.SP2
HRM-M14	number of performance reviews performed (by type)	performance evaluation	impl	base of type count	HRM:SG3.SP3
HRM-M15	percentage of staff that have resilience performance goals and objectives	performance evaluation	impl	derived	HRM:SG3.SP2
HRM-M16	percentage of staff that have met/not met their resilience performance goals and objectives	performance evaluation	impl	derived	HRM:SG3.SP2
HRM-M17	number of infractions referred to the incident management process	disciplinary action	impl	base of type count	HRM:SG3.SP4
HRM-M18	number of infractions requiring coordination with public authorities	disciplinary action	impl	base of type count	HRM:SG3.SP4

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
HRM-M19	number of violations of resilience policies subject to disciplinary action	disciplinary action; resilience policy compliance	impl	base of type count	HRM:SG3.SP4
HRM-M20	elapsed time since measures of resilience policy compliance were collected and reviewed	resilience policy compliance	impl	base of type schedule	HRM:SG3.SP4
HRM-M21	number of skill gaps referred to the risk management process	risk identification	impl	base of type count	HRM:SG1.SP3
HRM-M22	percentage of departing staff (from a position, from the organization) that participate in an exit interview	changes of employment status	impl	derived	HRM;SG4.SP1
HRM-M23	percentage of departing staff (from a position, from the organization) that have returned all organizational assets, property, and information	changes of employment status	impl	derived	HRM;SG4.SP2
HRM-M24	percentage of departing staff (from a position, from the organization) whose access rights have been discontinued as scheduled	changes of employment status	impl	derived	HRM;SG4.SP2
HRM-M25	percentage of involuntary terminations that are processed in accordance with established criteria and procedures	changes of employment status	impl	derived	HRM;SG4.SP3

Identity Management (ID)

The purpose of Identity Management is to create, maintain, and deactivate identities that may need some level of trusted access to organizational assets and to manage their associated attributes.

Summary of Specific Goals and Practices

ID:SG1 Establish Identities

- ID:SG1.SP1 Create Identities
- ID:SG1.SP2 Establish Identity Community
- ID:SG1.SP3 Assign Roles to Identities

ID:SG2 Manage Identities

- ID:SG2.SP1 Monitor and Manage Identity Changes
- ID:SG2.SP2 Periodically Review and Maintain Identities
- ID:SG2.SP3 Correct Inconsistencies
- ID:SG2.SP4 Deprovision Identities

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
ID-M1	elapsed time from identity request to granting of identity credentials	identity requests	effectiveness	base of type schedule	ID:SG1.SP1
ID-M2	percentage of identity requests denied (based on policy)	identity requests	impl	derived	ID:SG1.SP1

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
ID-M3	percentage of identity requests approved that, on further investigation, should have been denied based on, for example, a mismatch with designated roles	identity requests	effectiveness	derived	ID:SG2.SP2
ID-M4	percentage of identity requests that duplicate previous or current requests	identity requests	impl	derived	ID:SG1.SP1
ID-M5	percentage of identities for which roles have been authorized and justified by identity owners	identity roles	impl	derived	ID:SG1.SP3
ID-M6	rate of change requests to current identity profiles	identity profiles	impl	derived	ID:SG2.SP1
ID-M7	number of inconsistencies between identity profiles and their associated persons, objects, and entities	identity profiles; identity community	effectiveness	base of type count	ID:SG1.SP1 ID:SG2.SP1
ID-M8	percentage of identity profiles that are inaccurate	identity profiles	effectiveness	derived	ID:SG2.SP2
ID-M9	percentage of identity profiles that are vacant or invalid	identity profiles	effectiveness	derived	ID:SG2.SP2
ID-M10	percentage of identity profiles that are redundant	identity profiles	effectiveness	derived	ID:SG2.SP2
ID-M11	percentage of identity community inconsistencies for which corrective action is pending beyond schedule	identity profiles; identity community	impl	derived	ID:SG2.SP2 ID:SG2.SP3
ID-M12	percentage of identities belonging to external entities	identity community	impl	derived	ID:SG1.SP1
ID-M13	percentage of deprovisioned identities whose deprovisioning is pending beyond schedule	deprovisioning	impl	derived	ID:SG2.SP4
ID-M14	number of incidents involving the identity repository	identity repository; incident analysis	impl	base of type count	ID:SG1.SP2
ID-M15	number of incidents involving the identity repository for which resolution is pending beyond schedule	identity repository; incident analysis	impl	base of type defect	ID:SG1.SP2 IMC:SG4.SP2
ID-M16	number of identity-related risks referred to the risk management process	risk identification	impl	base of type count	ID:SG2.SP3

Incident Management and Control (IMC)

The purpose of Incident Management and Control is to establish processes to identify and analyze events, detect incidents, and determine an appropriate organizational response.

Summary of Specific Goals and Practices

IMC:SG1 Establish the Incident Management and Control Process

IMC:SG1.SP1 Plan for Incident Management

IMC:SG1.SP2 Assign Staff to the Incident Management Plan

IMC:SG2 Detect Events

IMC:SG2.SP1 Detect and Report Events

IMC:SG2.SP2 Log and Track Events

IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence

IMC:SG2.SP4 Analyze and Triage Events

IMC:SG3 Declare Incidents

IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria

IMC:SG3.SP2 Analyze Incidents

IMC:SG4 Respond to and Recover from Incidents

IMC:SG4.SP1 Escalate Incidents

IMC:SG4.SP2 Develop Incident Response

IMC:SG4.SP3 Communicate Incidents

IMC:SG4.SP4 Close Incidents

IMC:SG5 Establish Incident Learning

IMC:SG5.SP1 Perform Post-Incident Review

IMC:SG5.SP2 Integrate with the Problem Management Process

IMC:SG5.SP3 Translate Experience to Strategy

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
IMC-M1	percentage of coverage of IM plan (extent to which IM management plan includes all organizational units and functions that require coverage; aka IM plan scope)	IM planning	impl; possibly effectiveness	derived	IMC:SG1.SP1
IMC-M2	percentage of IM roles/responsibilities assigned to staff roles/members (extent to which IM plan roles and tasks are assigned to specific staff roles/members)	IM roles	impl	derived	IMC:SG1.SP2 IMC:SG2.SP1
IMC-M3	percentage of staff who have not been trained on their roles and responsibilities as defined in IM plans	IM training	impl	derived	IMC:SG1.SP2
IMC-M4	percentage of staff (managers, users) who have not completed training and awareness to identify anomalies and report them in the required timeframe (initial, refresher)	IM training	impl	derived	IMC:SG2.SP1
IMC-M5	percentage of events triaged (events reported vs. events analyzed)	event analysis	impl	derived	IMC:SG2.SP4
IMC-M6	percentage of events that are stalled or awaiting activity beyond threshold	event analysis	impl; possibly effectiveness	derived	IMC:SG2.SP1 IMC:SG2.SP2
IMC-M7	percentage of events whose documentation does not meet rules, laws, regulations, policies, or other requirements for forensic purposes	event analysis	impl	derived	IMC:SG2.SP3
IMC-M8	percentage of events without a disposition	event analysis	impl	derived	IMC:SG2.SP4
IMC-M9	percentage of events open beyond scheduled threshold (such as specified number of days for closure)	event analysis	impl	derived	IMC:SG2.SP4
IMC-M10	mean, median time to close an event, categorized in some meaningful manner	event analysis	impl; possibly effectiveness	derived	IMC:SG2.SP4

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
IMC-M11	percentage change in the number of logged events	event analysis	impl; possibly effectiveness	derived	IMC:SG2.SP2
IMC-M12	percentage of events that recur and result in declared incidents	incident analysis	impl; possibly effectiveness	derived	IMC:SG3.SP2 IMC:SG5.SP1
IMC-M13	percentage of events (or sets of related events) declared as incidents	incident analysis	impl	derived	IMC:SG3.SP2 IMC:SG5.SP1
IMC-M14	percentage of events declared as incidents that do not match the current incident declaration criteria	incident analysis	impl	derived	IMC:SG3.SP1
IMC-M15	number of incidents by incident type	incident analysis	impl	base of type count	IMC:SG3.SP2
IMC-M16	percentage of incidents that have been declared but not closed	incident analysis	impl	derived	IMC:SG3.SP2 IMC:SG4.SP4
IMC-M17	percentage of incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds	incident analysis	impl	derived	IMC:SG3.SP2 IMC:SG5.SP1
IMC-M18	percentage of operational time that services and assets were unavailable (as seen by users and customers) due to incidents	incident analysis	effectiveness	derived	IMC:SG5.SP1
IMC-M19	number of incidents by incident type and impact[33]	incident analysis	impl	base of type count	IMC:SG5.SP1
IMC-M20	number of incidents by incident type and root cause	incident analysis	impl	base of type count	IMC:SG5.SP1
IMC-M21	impact due to incidents by incident type	incident analysis	impl	derived	IMC:SG5.SP1
IMC-M22	change in impact due to incidents by incident type	incident analysis	impl; possibly effectiveness	derived	IMC:SG5.SP1
IMC-M23	percentage of incidents that recur	incident analysis	impl; possibly effectiveness	derived	IMC:SG3.SP2 IMC:SG5.SP1
IMC-M24	percentage change in the number of incidents by incident type	incident analysis	impl; possibly effectiveness	derived	IMC:SG5.SP1
IMC-M25	time (mean, median, range) between event detection and related incident declaration	incident analysis	impl; possibly effectiveness	derived	IMC:SG5.SP1
IMC-M26	time (mean, median, range) between event detection and related incident response	incident analysis	impl; possibly effectiveness	derived	IMC:SG5.SP1
IMC-M27	time (mean, median, range) between event detection and related incident closure	incident analysis	impl; possibly effectiveness	derived	IMC:SG5.SP1
IMC-M28	percentage change in the elapsed time of the incident life cycle by incident type (mean, median, ranges)	incident analysis	impl; possibly effectiveness	derived	IMC:SG5.SP1

[33] Impact (i.e., the magnitude or consequences due to incidents) can be represented as monetary cost, productivity cost, loss of revenue due to unavailability of services, etc.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
IMC-M29	percentage of incidents that result in realized risks that exceed established risk parameters	incident risk	impl; possibly effectiveness	derived	none
IMC-M30	percentage of incidents that require escalation	incident escalation	impl	derived	IMC:SG4.SP1
IMC-M31	percentage of incidents that require involvement of law enforcement[34]	incident escalation	impl; possibly effectiveness	derived	IMC:SG4.SP3
IMC-M32	percentage of incidents that require the involvement of regulatory and governing agencies	incident escalation	impl; possibly effectiveness	derived	IMC:SG4.SP3
IMC-M33	percentage of post-incident review recommendations that result in control changes or improvements to the process	process improvement	impl	derived	IMC:SG5.SP1
IMC-M34	number of problem reports referred to the problem management system	process improvement	impl	base of type count	IMC:SG5.SP2
IMC-M35	extent to which incident occurrence (prevent) is reduced as a result of implementing RMM appraisal findings	potential element of resilience posture	effectiveness	derived	none
IMC-M36	reduction in incident occurrence and impact (detect, respond, recover) as a result of implementing CERT-RMM appraisal findings	potential element of resilience posture	effectiveness	derived	none

Knowledge and Information Management (KIM)

The purpose of Knowledge and Information Management is to establish and manage an appropriate level of controls to support the confidentiality, integrity, and availability of the organization's information, vital records, and intellectual property.

Summary of Specific Goals and Practices

KIM:SG1 Establish and Prioritize Information Assets

KIM:SG1.SP1 Prioritize Information Assets

KIM:SG1.SP2 Categorize Information Assets

KIM:SG2 Protect Information Assets

KIM:SG2.SP1 Assign Resilience Requirements to Information Assets

KIM:SG2.SP2 Establish and Implement Controls

KIM:SG3 Manage Information Asset Risk

KIM:SG3.SP1 Identify and Assess Information Asset Risk

KIM:SG3.SP2 Mitigate Information Asset Risk

KIM:SG4 Manage Information Asset Confidentiality and Privacy

KIM:SG4.SP1 Encrypt High-Value Information

KIM:SG4.SP2 Control Access to Information Assets

KIM:SG4.SP3 Control Information Asset Disposition

[34] Could include additional measures here for any of the roles listed in IMC:SG4.SP3

KIM:SG5 Manage Information Asset Integrity

KIM:SG5.SP1 Control Modification of Information Assets

KIM:SG5.SP2 Manage Information Asset Configuration

KIM:SG5.SP3 Verify Validity of Information

KIM:SG6 Manage Information Asset Availability

KIM:SG6.SP1 Perform Information Duplication and Retention

KIM:SG6.SP2 Manage Organizational Knowledge

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
KIM-M1	percentage of information assets that have been inventoried	asset inventory	impl	derived	ADM:SG1.SP1 KIM:SG1.SP1
KIM-M2	percentage of information assets with/without a complete asset profile (such as no stated resilience requirements)	asset inventory	impl	derived	ADM:SG1.SP2 KIM:SG2.SP1
KIM-M3	percentage of information assets with/without a designated owner	asset inventory	impl	derived	ADM:SG1.SP3
KIM-M4	percentage of information assets with/without a designated custodian (if applicable)	asset inventory	impl	derived	ADM:SG1.SP3
KIM-M5	percentage of information assets that have designated owners but no custodians (if applicable)	asset inventory	impl	derived	ADM:SG1.SP3
KIM-M6	percentage of information assets that have designated custodians but no owners	asset inventory	impl	derived	ADM:SG1.SP3
KIM-M7	percentage of information assets that have been inventoried, by service	asset inventory	impl	derived	ADM:SG2.SP1
KIM-M8	percentage of information assets that are not associated with one or more services	asset inventory	impl	derived	ADM:SG2.SP1
KIM-M9	elapsed time since the information asset inventory was reviewed	asset inventory	impl	base of type schedule	ADM:SG1.SP1 ADM:SG3.SP1
KIM-M10	percentage of information asset-service dependency conflicts with unimplemented or incomplete mitigation plans	asset-service dependencies	impl	derived	ADM:SG2.SP2
KIM-M11	percentage of information asset-service dependency conflicts with no mitigation plan	asset-service dependencies	impl	derived	ADM:SG2.SP2
KIM-M12	number of discrepancies between the current inventory and the previous inventory	asset inventory	impl	base of type count	ADM:SG3.SP1
KIM-M13	number of changes made to asset profiles in the information asset inventory	asset inventory	impl	base of type count	ADM:SG3.SP2
KIM-M14	number of changes to resilience requirements as a result of information asset changes	asset change management	impl	base of type count	ADM:SG3.SP2
KIM-M15	number of changes to service continuity plans as a result of information asset changes	asset change management	impl	base of type count	ADM:SG3.SP2
KIM-M1	percentage of information assets that are designated as high-value assets	asset inventory	impl	derived	KIM:SG1.SP1

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
KIM-M16	elapsed time since review and validation of high-value information assets and their priorities	asset inventory	impl	derived	KIM:SG1.SP1
KIM-M17	number of information assets categorized by service (includes number of assets that support 2 or more, 3 or more, etc., services)	asset inventory	impl	base of type count	KIM:SG1.SP1
KIM-M18	percentage of information assets that have not been categorized as to level of sensitivity	asset inventory	impl	derived	KIM:SG1.SP2
KIM-M19	percentage of information assets without assigned/defined resilience requirements	asset requirements	impl	derived	KIM:SG2.SP1
KIM-M20	percentage of information assets with assigned/defined resilience requirements that are undocumented	asset requirements	impl	derived	KIM:SG2.SP1
KIM-M21	percentage of information assets with no (or missing) protection controls	asset controls	impl; possibly effectiveness	derived	KIM:SG2.SP2
KIM-M22	percentage of information assets with no (or missing) sustainment controls	asset controls	impl; possibly effectiveness	derived	KIM:SG2.SP2
KIM-M23	percentage of information asset controls (protection and sustainment) that are ineffective or inadequate as demonstrated by: unsatisfied control objectives unmet resilience requirements outstanding control assessment problem areas above established thresholds and without remediation plans	asset controls	impl; possibly effectiveness	derived	KIM:SG2.SP2
KIM-M24	percentage of information asset control deficiencies not resolved by scheduled due date (refer to CTRL measures for categories of control deficiencies)	asset controls	impl	derived	KIM:SG2.SP2
KIM-M25	elapsed time since review of the effectiveness of information asset controls	asset controls	impl	base of type schedule	KIM:SG2.SP2
KIM-M26	elapsed time since risk assessment of information assets performed	asset risk	impl	base of type schedule	KIM:SG3.SP1
KIM-M27	elapsed time since business impact analysis of information assets performed	asset risk	impl	base of type schedule	KIM:SG3.SP1
KIM-M28	percentage of information assets for which business impact valuation[35] has not been performed	asset risk	impl	derived	KIM:SG3.SP1
KIM-M29	percentage of information assets for which a risk assessment has not been performed and documented (per policy or other guideline) and according to plan	asset risk	impl	derived	KIM:SG3.SP1
KIM-M30	percentage of information asset risks that have not been assigned to a responsible party for action, tracking, and closure	asset risk	impl	derived	KIM:SG3.SP2

[35] Business impact valuation can be either qualitative (high, medium, low) or quantitative (based on levels of loss or damage, fines, number of customers lost, disruption in access, disclosure, alteration, destruction, etc.).

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
KIM-M31	percentage of information asset risks[36] with a disposition of "mitigate or control" that do not have a defined mitigation plan	asset risk	impl	derived	KIM:SG3.SP2[37]
KIM-M32	percentage of information asset risks with a "mitigate or control" disposition that are not effectively mitigated by their mitigation plans	asset risk	effective-ness	derived	KIM:SG3.SP2
KIM-M33	percentage of realized risks for information assets that exceed established risk para-meters	asset risk	effective-ness	derived	KIM:SG3.SP2
KIM-M34	number of violations of access control policies for information assets as a result, number of successful intru-sions to technology assets (digital informa-tion assets) or facility assets (physical information assets) where information assets "live" as a result, number of information assets that have been accessed in an unautho-rized manner as a result, number of incidents declared as a result, number of breaches of confi-dentiality and privacy	asset intru-sions; asset integrity	impl; pos-sibly effec-tiveness	base of type count	KIM:SG4.SP2 KIM:SG5.SP1
KIM-M35	percentage of information assets for which encryption is required and not imple-mented	asset inven-tory; asset confidentiali-ty	impl	derived	KIM:SG4.SP1
KIM-M36	percentage of retired information assets that are not disposed of in accordance with information asset disposition guide-lines	asset confi-dentiality	impl	derived	KIM:SG4.SP3
KIM-M37	percentage of retired information assets that have not been disposed according to plan	asset confi-dentiality	impl	derived	KIM:SG4.SP3
KIM-M38	percentage of anomalies in information asset modification logs that have not been addressed as scheduled	asset integri-ty	impl	derived	KIM:SG5.SP1
KIM-M39	percentage of anomalies in information asset configuration control logs that have not been addressed as scheduled	asset integri-ty	impl	derived	KIM:SG5.SP2
KIM-M40	percentage of information asset logs which are not validated and placed under configuration control as scheduled	asset integri-ty	impl	derived	KIM:SG5. SP1 KIM:SG5.SP2 KIM:SG5.SP3
KIM-M41	percentage of information assets with accuracy and completeness controls that have not been reviewed as scheduled	asset integri-ty	impl	derived	KIM:SG5.SP3
KIM-M42	percentage of information assets that have not been backed up as scheduled	asset availa-bility	impl	derived	KIM:SG6.SP1

[36] This measure also appears in RISK M4-1. For ease of use of an individual PA (vs. ease of maintenance and consistency), we have decided to replicate some (but not all) risk-related measures in the individual asset PAs that are identified generally in the list of RISK PA measures.

[37] SG3.SP2 subpractice 7 states, "Collect performance measures on the risk management process." No such measures are included here in KIM; refer to the RISK PA.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
KIM-M43	percentage of information assets that have not been tested to verify that they can be accurately restored from backups as scheduled	asset availability	impl	derived	KIM:SG6.SP1
KIM-M44	percentage of vital staff with institutional knowledge where such knowledge has not been captured/transferred (via such methods as cross training)	asset availability	impl	derived	KIM:SG6.SP2
KIM-M45	percentage of information assets that do not satisfy their resilience requirements	asset evaluation	impl; possibly effectiveness	derived	KIM:SG4, SG5, SG6
KIM-M46	number of policy violations related to confidentiality, integrity, availability, privacy, and access control of information assets	asset evaluation	impl	base of type count	none
KIM-M47	percentage of external entities that are not meeting service level agreements for information assets subject to external entity services	asset evaluation	impl	derived	none
KIM-M48	percentage of information assets that are not maintained at required maintenance levels (for information assets subject to maintenance agreements)	asset evaluation	impl	derived	none

Measurement and Analysis (MA)

The purpose of Measurement and Analysis is to develop and sustain a measurement capability that is used to support management information needs for managing the operational resilience management system.

Summary of Specific Goals and 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

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
MA-M1	percentage of measurement objectives that can be traced to information needs and objectives	measurement objectives	impl	derived	MA:SG1.SP1
MA-M2	percentage of measures for which operational definitions have been specified	measures	impl	derived	MA:SG1.SP2

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
MA-M3	percentage of measurement objectives achieved (against defined targets, if relevant)	measurement objectives	effectiveness	derived	MA:SG2.SP2
MA-M4	percentage of operational resilience management system performance goals for which measurement data is collected, analyzed, and communicated	ORMS measurement	impl	derived	MA:SG2.SP1 MA:SG2.SP2 MA:SG2.SP4
MA-M5	percentage of organizational units, services, and activities using operational resilience management measures to assess the performance of operational resilience management processes	ORMS measurement	impl; possibly effectiveness	derived	MA:SG2.SP4
MA-M6	elapsed time between collection, analysis, and communication of measurement data	measurement process	impl	base of type schedule	MA:SG2.SP1 MA:SG2.SP2 MA:SG2.SP4
MA-M7	percentage of measures that can be traced to measurement objectives	measurement process	impl	derived	MA:SG1.SP1 MA.SG2.SP1
MA-M8	percentage of measures whose collection, analysis, and reporting is automated	measurement process	impl	derived	MA.SG2.SPI MA.SG2.SP2 MA.SG2.SP3
MA-M9	percentage of specified measures that are collected, analyzed, and stored	measures	impl	derived	MA:SG1.SP3 MA:SG1.SP4 MA:SG2.SP1 MA:SG2.SP2 MA:SG2.SP3

Monitoring (MON)

The purpose of Monitoring is to collect, record, and distribute information about the operational resilience management system to the organization on a timely basis.

Summary of Specific Goals and Practices

MON:SG1 Establish and Maintain a Monitoring Program

MON:SG1.SP1 Establish a 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

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
MON-M1	percentage of operational resilience management system performance goals for which monitoring data is collected, recorded, and distributed	ORMS assessment	impl	derived	MON:SG2.SP3 MON:SG2.SP4

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
MON-M2	percentage of organizational units, services, and activities using monitoring data to assess the performance of operational resilience management processes	ORMS assessment	process performance	derived	none
MON-M3	percentage of monitoring requirements accepted (accepted requirements divided by total requirements)	monitoring coverage	impl	derived	MON:SG1.SP3 MON:SG1.SP4
MON-M4	number of requirements gaps (total requirements minus accepted requirements)	monitoring coverage	impl	base of type count	MON:SG1.SP3 MON:SG1.SP4
MON-M5	number of ranked risks resulting from unsatisfied monitoring requirements	risk identification	impl	base of type count	MON:SG1.SP4
MON-M6	elapsed time from high-value data collection to data distribution to key stakeholders	monitoring communication	effectiveness	base of type schedule	MON:SG2.SP4
MON-M7	number of new, changed, and retired monitoring requirements	monitoring variability	impl	base of type count	MON:SG1.SP3
MON-M8	number of times monitoring plan has been revised	monitoring variability	impl	base of type count	MON:SG1.SP1
MON-M9	percentage of data collection activities that are automated	monitoring process	impl	derived	MON:SG2.SP3

Organization Process Definition (OPD)

The purpose of Organizational Process Definition is to establish and maintain a usable set of organizational process assets and work environment standards for operational resilience.

Summary of Specific Goals and Practices

OPD:SG1 Establish Organizational Process Assets

- OPD:SG1.SP1 Establish Standard Processes
- OPD:SG1.SP2 Establish Tailoring Criteria and Guidelines
- OPD:SG1.SP3 Establish the Organization's Measurement Repository
- OPD:SG1.SP4 Establish the Organization's Process Asset Library
- OPD:SG1.SP5 Establish Work Environment Standards
- OPD:SG1.SP6 Establish Rules and Guidelines for Integrated Teams

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
OPD-M1	percentage of organizational units (including projects) using the organization's standard processes	standard process deployment	impl	derived	OPD:SG1.SP1
OPD-M2	percentage of standard processes that map to process policies, standards, or models	standard process development	impl	derived	OPD:SG1.SP1

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
OPD-M3	percentage of standard processes that satisfy process needs and objectives	standard process development	impl	derived	OPD:SG1.SP1
OPD-M4	percentage of standard processes that have been peer reviewed	standard process development	impl	derived	OPD:SG1.SP1
OPD-M5	percentage of standard processes that have been tailored, by organizational unit	standard process use	impl	derived	OPD:SG1.SP2
OPD-M6	number of times a standard process has been tailored	standard process use	impl	base of type count	OPD:SG1.SP2
OPD-M7	number of waivers by standard process	standard process deployment	impl	base of type count	OPD:SG1.SP2
OPD-M8	percentage of tailoring guidelines that have been peer reviewed	tailoring guideline development	impl	derived	OPD:SG1.SP2
OPD-M9	defect density of each process element of the organization's set of standard processes	standard process development	effectiveness	derived	OPD:SG1.SP1
OPD-M10	elapsed time for development of a standard process (mean, median)	standard process development	impl	base of type schedule	OPD:SG1.SP1
OPD-M11	elapsed time for changes to a standard process (mean, median)	standard process maintenance	impl	base of type schedule	OPD:SG1.SP1
OPD-M12	number of unapproved changes to the process asset library	process asset maintenance	impl	base of type count	OPD:SG1.SP4
OPD-M13	number of times each item in the process assets library is accessed	process asset library use	impl	base of type count	OPD:SG1.SP4
OPD-M14	percentage of product and process measures residing in the measurement repository that are used in status reports	measurement repository	impl	derived	OPD:SG1.SP3
OPD-M15	number of waivers by work environment standard	work environment standards	impl	base of type count	OPD:SG1.SP5
OPD-M16	number of worker's compensation claims due to work environment	work environment standards	impl	base of type count	OPD:SG1.SP5

Organizational Process Focus (OPF)

The purpose of Organizational Process Focus is to plan, implement, and deploy organizational process improvements based on a thorough understanding of current strengths and weaknesses of the organization's operational resilience processes and process assets.

Summary of Specific Goals and Practices

OPF:SG1 Determine Process Improvement Opportunities

OPF:SG1.SP1 Establish Organizational Process Needs

OPF:SG1.SP2 Appraise the Organization's Processes

OPF:SG1.SP3 Identify the Organization's Process Improvements

OPF:SG2 Plan and Implement Process Actions

OPF:SG2.SP1 Establish Process Action Plans

OPF:SG2.SP2 Implement Process Action Plans

OPF:SG3 Deploy Organizational Process Assets and Incorporate Experiences

OPF:SG3.SP1 Deploy Organizational Process Assets

OPF:SG3.SP2 Deploy Standard Processes

OPF:SG3.SP3 Monitor the Implementation

OPF:SG3.SP4 Incorporate Experiences into Organizational Process Assets

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
OPF-M1	percentage of process improvement proposals accepted	process improvement	impl	derived	OPF:SG1.SP3
OPF-M2	percentage of planned process improvements implemented	process improvement	impl	derived	OPF:SG2.SP2
OPF-M3	percentage of improvements resulting from appraisals	process improvement	impl	derived	OPF:SG1.SP2 OPF:SG1.SP3
OPF-M4	percentage of improvements resulting from experience reports and lessons learned	process improvement	impl	derived	OPF:SG1.SP3 OPF:SG3.SP4
OPF-M5	CERT Resilience Management Model capability levels	process capability	effectiveness	derived	OPF:SG1.SP2
OPF-M6	elapsed time for deployment of an organizational process asset	process asset deployment	impl	base of type schedule	OPF:SG3.SP1
OPF-M7	status against schedule for deployment of an organizational process asset (i.e., met or exceeded and by how much)	process asset deployment	effectiveness	derived	OPF:SG3.SP1
OPF-M8	percentage of organizational units using the organization's current set of standard processes (or tailored versions of same)	standard process deployment	impl	derived	OPF:SG3.SP2
OPF-M9	issue trends associated with implementing the organization's set of standard processes (i.e., number of issues identified and number closed)	standard process deployment	effectiveness	derived	OPF:SG3.SP3
OPF-M10	percentage of waivers approved/rejected by standard process	standard process deployment	impl	derived	OPF:SG3.SP4
OPF-M11	percentage of standard processes that have been tailored, by organizational unit	standard process tailoring	impl	derived	OPF:SG3.SP2

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
OPF-M12	number of times a standard process has been tailored	standard process use	impl	base of type count	OPF:SG3.SP4
OPF-M13	progress toward achievement of process needs and objectives	process objectives	effective-ness	derived	OPF:SG1.SP1
OPF-M14	percentage of processes that can be mapped directly to documented critical success factors or an enterprise strategy	process objectives	impl	derived	OPF:SG1.SP1

Organization Training and Awareness (OTA)

The purpose of Organizational Training and Awareness is to promote awareness in and develop skills and knowledge of people in support of their roles in attaining and sustaining operational resilience.

Summary of Specific Goals and Practices

OTA:SG1 Establish Awareness Program

- OTA:SG1.SP1 Establish Awareness Needs
- OTA:SG1.SP2 Establish Awareness Plan
- OTA:SG1.SP3 Establish Awareness Delivery Capability

OTA:SG2 Conduct Awareness Activities

- OTA:SG2.SP1 Perform Awareness Activities
- OTA:SG2.SP2 Establish Awareness Records
- OTA:SG2.SP3 Assess Awareness Program Effectiveness

OTA:SG3 Establish Training Capability

- OTA:SG3.SP1 Establish Training Needs
- OTA:SG3.SP2 Establish Training Plan
- OTA:SG3.SP3 Establish Training Capability

OTA:SG4 Conduct Training

- OTA:SG4.SP1 Deliver Training
- OTA:SG4.SP2 Establish Training Records
- OTA:SG4.SP3 Assess Training Effectiveness

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
OTA-M1	percentage of awareness needs for each staff group that are addressed in the awareness plan	awareness needs; aware-ness activities	impl	derived	OTA:SG1.SP1 OTA:SG1.SP2
OTA-M2	difference in planned versus actual awareness sessions delivered	awareness activities	impl	derived	OTA:SG1.SP2 OTA:SG2.SP1
OTA-M3	schedule of delivery of awareness ses-sions (planned frequency versus actual frequency)	awareness activities	impl	derived	OTA:SG1.SP2 OTA:SG2.SP1

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
OTA-M4	elapsed time since awareness materials were reviewed and updated	awareness activities	impl	base of type schedule	OTA:SG1.SP3
OTA-M5	percentage of new users (internal and external) who have satisfactorily completed awareness sessions before being granted network access	awareness activities; awareness requirements	impl	derived	OTA:SG2.SP2
OTA-M6	percentage of users (internal and external) who have satisfactorily completed periodic awareness refresher sessions as required by policy	awareness activities; awareness requirements	impl	derived	OTA:SG2.SP2
OTA-M7	percentage of awareness activities that include a mechanism for evaluating the effectiveness of the awareness activity	awareness activities	impl	derived	OTA:SG2.SP3
OTA-M8	percentage of passing scores (by participants) on awareness assessments	awareness assessments	effectiveness	derived	OTA:SG2.SP3
OTA-M9	percentage of staff who have been assessed to determine if their level of awareness is commensurate with their job responsibilities	awareness assessments	effectiveness	derived	OTA:SG2.SP3
OTA-M10	percentage of staff waived from awareness activities	awareness waivers	impl	derived	OTA:SG2.SP2
OTA-M11	percentage of training needs for each role and responsibility that are addressed in the training plan	training needs; training courses	impl	derived	OTA:SG3.SP1 OTA:SG3.SP2
OTA-M12	difference in planned versus actual training courses delivered	training courses	impl	derived	OTA:SG3.SP2 OTA:SG4.SP1
OTA-M13	schedule of delivery of training sessions (planned frequency versus actual frequency)	training courses	impl	derived	OTA:SG3.SP2 OTA:SG4.SP1
OTA-M14	percentage of favorable post-training evaluation ratings, including instructor ratings	training courses	effectiveness	derived	OTA:SG4.SP3
OTA-M15	elapsed time since training materials were reviewed and updated	training materials	impl	base of type schedule	OTA:SG3.SP3
OTA-M16	number of internal staff members for whom training was planned versus number trained (percentage)	staff training	impl	derived	OTA:SG4.SP1
OTA-M17	number of external staff members for whom training was expected or contracted versus number trained (percentage)	staff training	impl	derived	OTA:SG4.SP1
OTA-M18	percentage of favorable training program quality survey ratings	training program	effectiveness	derived	OTA:SG4.SP3
OTA-M19	percentage of passing scores (by participants) on training examinations	training examinations	effectiveness	derived	OTA:SG4.SP2
OTA-M20	percentage of staff who have been assessed to determine if training has been effective[38] commensurate with their job responsibilities	training assessment	effectiveness	derived	OTA:SG4.SP3
OTA-M21	percentage of staff waived from training	training waivers	impl	derived	OTA:SG4.SP2

[38] OTA:SG4.SP3 provides several approaches for assessing training effectiveness.

People Management (PM)

The purpose of People Management is to establish and manage the contributions and availability of people to support the resilient operation of organizational services.

Summary of Specific Goals and Practices

PM:SG1 Establish Vital Staff

PM:SG1.SP1 Identify Vital Staff

PM:SG2 Manage Risks Associated with Staff Availability

PM:SG2.SP1 Identify and Assess Staff Risk

PM:SG2.SP2 Mitigate Staff Risk

PM:SG3 Manage the Availability of Staff

PM:SG3.SP1 Establish Redundancy for Vital Staff

PM:SG3.SP2 Perform Succession Planning

PM:SG3.SP3 Prepare for Redeployment

PM:SG3.SP4 Plan to Support Staff During Disruptive Events

PM:SG3.SP5 Plan for Return-to-Work Considerations

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
PM-M1	percentage of staff-service dependency conflicts with unimplemented or incomplete mitigation plans	asset-service dependencies; risk mitigation	impl	derived	ADM:SG2.SP2 PM:SG2.SP1 PM:SG2.SP2
PM-M2	percentage of staff-service dependency conflicts with no mitigation plan	asset-service dependencies; risk mitigation	impl	derived	ADM:SG2.SP2 PM:SG2.SP1 PM:SG2.SP2
PM-M3	number of changes to service continuity plans as a result of staff changes	asset change management; SC plans	impl	base of type count	ADM:SG3.SP2
PM-M4	percentage of staff and managers that are designated as vital	asset inventory; vital staff; vital managers	impl	derived	ADM:SG1.SP1 PM:SG1.SP1
PM-M5	elapsed time since the list of vital staff has been reviewed and reconciled with service continuity plans	asset inventory; vital staff	impl	base of type schedule	PM:SG1.SP1
PM-M6	percentage of vital staff for which some form of risk assessment of staff availability has not been performed and documented (per policy or other guideline) within the specified timeframe	asset risk	impl	derived	PM:SG2.SP1
PM-M7	percentage of vital staff availability risks that have not been assigned to a responsible party for action, tracking, and closure	asset risk	impl	derived	PM:SG2.SP2
PM-M8	percentage of vital staff availability risks with a disposition of “mitigate or control” that do not have a defined mitigation plan	asset risk	impl	derived	PM:SG2.SP2[39]

[39] SG3.SP2 subpractice 7 states, “Collect performance measures on the risk management process.” No such measures are included here in PM; refer to the RISK PA.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
PM-M9	percentage of vital staff availability risks with a “mitigate or control” disposition that are not effectively mitigated by their mitigation plans	asset risk	impl	derived	PM:SG2.SP2
PM-M10	percentage of realized risks on the availability of vital staff that have exceeded established risk parameters	asset risk	effectiveness	derived	PM:SG2.SP2
PM-M11	percentage of vital staff who do not have redundancy plans	vital staff; redundancy plans	impl	derived	PM:SG3.SP1
PM-M12	cost required to address training gaps for those designated as backups and replacements for vital staff	vital staff; training gaps	impl	base of type cost	PM:SG3.SP1
PM-M13	elapsed time required to address training gaps for those designated as backups and replacements for vital staff	vital staff; training gaps	impl	base of type schedule	PM:SG3.SP1
PM-M14	effort required to address training gaps for those designated as backups and replacements for vital staff	vital staff; training gaps	impl	base of type effort	PM:SG3.SP1
PM-M15	percentage of vital staff available (on hand) to conduct service continuity planned exercises and tests (versus those needed)	vital staff; SC tests	impl	derived	SC:SG5.SP3
PM-M16	percentage of vital staff not covered by a service continuity plan	vital staff; SC plans	impl	derived	PM:SG3.SP3
PM-M17	percentage of vital staff who have not been trained for redeployment	vital staff; SC plans	impl	derived	PM:SG3.SP3
PM-M18	percentage of vital managers who do not have succession plans	vital managers; succession plans	impl	derived	PM:SG3.SP2
PM-M19	number of reports to public authorities regarding the loss of a vital higher level manager	vital managers	impl	base of type count	none
PM-M20	percentage of first responders who do not have appropriate credentials	first responders	impl	derived	PM:SG3.SP3
PM-M21	percentage of service continuity plans that do not include plans to support staff who are deployed during disruptive events	vital staff; SC plans	impl	derived	PM:SG3.SP4 SC:SG3.SP2
PM-M22	percentage of service continuity plans that do not include plans for transitioning staff back to the workplace (return to work)	vital staff; SC plans	impl	derived	PM:SG3.SP5 SC:SG3.SP2
PM-M23	number of people availability risks referred to the risk management process	vital staff; vital managers; risk identification	impl	base of type count	PM:SG2.SP1

Risk Management (RISK)

The purpose of Risk Management is to identify, analyze, and mitigate risks to organizational assets that could adversely affect the operation and delivery of services.

Summary of Specific Goals and Practices

RISK:SG1 Prepare for Risk Management

RISK:SG1.SP1 Determine Risk Sources and Categories

RISK:SG1.SP2 Establish an Operational Risk Management Strategy

RISK:SG2 Establish Risk Parameters and Focus

RISK:SG2.SP1 Define Risk Parameters

RISK:SG2.SP2 Establish Risk Measurement Criteria

RISK:SG3 Identify Risk

RISK:SG3.SP1 Identify Asset-Level Risks

RISK:SG3.SP2 Identify Service-Level Risks

RISK:SG4 Analyze Risk

RISK:SG4.SP1 Evaluate Risk

RISK:SG4.SP2 Categorize and Prioritize Risk

RISK:SG4.SP3 Assign Risk Disposition

RISK:SG5 Mitigate and Control Risk

RISK:SG5.SP1 Develop Risk Mitigation Plans

RISK:SG5.SP2 Implement Risk Strategies

RISK:SG6 Use Risk Information to Manage Resilience

RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services

RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services

Measures

ID	Measure	Type of Information	Measure Type	Base vs. Derived	Applicable SG.SP
RISK-M1	number of internal operational risk sources identified	risk planning	impl	base of type count	RISK:SG1.SP1
RISK-M2	number of external operational risk sources identified	risk planning	impl	base of type count	RISK:SG1.SP1
RISK-M3	number of operational risk sources that are not addressed by process policies or other mitigating activities	risk sources	effec-tiveness	base of type count	RISK:SG1.SP1
RISK-M4	number of risk categories defined	risk planning	impl	base of type count	RISK:SG1.SP1
RISK-M5	elapsed time since validation of risk catego-ries performed	risk planning	impl	base of type schedule	RISK:SG1.SP1
RISK-M6	percentage of repeat audit findings related to operational risk management	risk strategy	impl	derived	RISK:SG1.SP2
RISK-M7	number of operational risks referred to the organization's enterprise risk management process	risk strategy	impl	base of type count	RISK:SG1.SP2
RISK-M8	number of risk parameters defined	risk strategy	impl	base of type count	RISK:SG2.SP1
RISK-M9	elapsed time since validation of risk parame-ters performed	risk strategy	impl	base of type schedule	RISK:SG2.SP1
RISK-M10	number of risk criteria defined	risk strategy	impl	base of type count	RISK:SG2.SP2
RISK-M11	elapsed time since validation of risk criteria performed	risk strategy	impl	base of type schedule	RISK:SG2.SP2

ID	Measure	Type of Information	Measure Type	Base vs. Derived	Applicable SG.SP
RISK-M12	elapsed time since risk assessment performed	asset risk	impl	base of type schedule	RISK:SG3.SP1
RISK-M13	elapsed time since business impact analysis performed	asset risk	impl	base of type schedule	RISK:SG3.SP1
RISK-M14	percentage of assets for which some form of risk assessment has not been performed and documented (per policy or other guideline) within the specified timeframe	risk assessment	impl	derived	RISK:SG3.SP1
RISK-M15	percentage of services for which some form of risk assessment of associated assets has not been performed and documented (per policy or other guideline)	risk assessment	impl	derived	RISK:SG3.SP2
RISK-M16	confidence factor that all risks that need to be identified have been identified (refer to template in [Allen 2010])	risk identification	effectiveness	derived	RISK:SG3.SP1 RISK:SG3.SP2
RISK-M17	change in number of identified risks that exceed risk parameters and measurement criteria	risk identification; risk valuation	impl	derived	RISK:SG3.SP1 RISK:SG3.SP2 RISK:SG4.SP2
RISK-M18	percentage of risks for which the impact (refer to RISK:SG2.SP2) has not been characterized (qualitative, quantitative)	risk valuation	impl	derived	RISK:SG4.SP1
RISK-M19	percentage of risks that have not been categorized and prioritized	risk categorization; risk prioritization	impl	derived	RISK:SG4.SP2
RISK-M20	percentage of risks that have been characterized as “high” impact according to risk parameters (refer to RISK:SG2)	risk valuation	impl	derived	RISK:SG4.SP1
RISK-M21	percentage of risks that exceed established risk parameters and measurement criteria, by risk category	risk valuation; risk categorization	impl	derived	RISK:SG4.SP1 RISK:SG4.SP2
RISK-M22	percentage of risks that do not have a documented and approved risk disposition	risk disposition	impl	derived	RISK:SG4.SP3
RISK-M23	percentage of risks that have not been assigned to a responsible party for action, tracking, and closure	risk mitigation	impl	derived	RISK:SG5.SP1
RISK-M24	percentage of previously identified risks that have converted from any other risk disposition to a risk disposition of “mitigate or control”	risk disposition	impl	derived	RISK:SG4.SP3
RISK-M25	percentage of risks with a disposition of “mitigate or control” that do not have a defined mitigation plan	risk disposition; risk mitigation	impl	derived	RISK:SG5.SP1
RISK-M26	percentage of 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; risk status	impl	derived	RISK:SG5.SP1 RISK:SG5.SP2
RISK-M27	percentage of services with an implemented mitigation plan	risk mitigation; risk status	impl	derived	RISK:SG5.SP1 RISK:SG5.SP2
RISK-M28	percentage of risks with a “mitigate or control” disposition with mitigations[40] that are not yet started	risk mitigation; risk status	impl	derived	RISK:SG5.SP2 RISK:SG6.SP1 RISK:SG6.SP2

[40] Including controls and updates to SC plans

ID	Measure	Type of Information	Measure Type	Base vs. Derived	Applicable SG.SP
RISK-M29	percentage of risks with a "mitigate or control" disposition with mitigations that are in progress (vs. completely implemented)	risk mitigation; risk status	impl	derived	RISK:SG5.SP2 RISK:SG6.SP1 RISK:SG6.SP2
RISK-M30	percentage of risks with a "mitigate or control" disposition that are not effectively mitigated by their mitigation plans	risk mitigation; risk status	effectiveness	base of type ordinal/ratio	RISK:SG5.SP2
RISK-M31	percentage of open risks that have not been tracked to closure	risk status	impl	derived	RISK:SG5.SP2
RISK-M32	percentage of risks with a disposition of "mitigate or control" that have a defined mitigation plan but whose status is not regularly reported (per policy or other guideline)	risk status	impl	derived	RISK:SG5.SP2
RISK-M33	percentage of realized risks that exceed established risk parameters[41]	risk status	effectiveness	derived	refer to comparable measures in EC, EXD, IMC, KIM, TM
RISK-M34	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 type schedule	RISK:SG5.SP2

Resilience Requirement Development (RRD)

The purpose of Resilience Requirements Development is to identify, document, and analyze the operational resilience requirements for high-value services and related assets.

Summary of Specific Goals and Practices

RRD:SG1 Identify Enterprise Requirements

RRD:SG1.SP1 Establish Enterprise Resilience Requirements

RRD:SG2 Develop Service Requirements

RRD:SG2.SP1 Establish Asset Resilience Requirements

RRD:SG2.SP2 Assign Enterprise Resilience Requirements to Services

RRD:SG3 Analyze and Validate Requirements

RRD:SG3.SP1 Establish a Definition of Required Functionality

RRD:SG3.SP2 Analyze Resilience Requirements

RRD:SG3.SP3 Validate Resilience Requirements

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
RRD-M1	percentage of enterprise requirements that have been communicated to all organizational units and lines of business	enterprise requirements	impl	derived	RRD:SG1.SP1
RRD-M2	percentage of services with incomplete or no stated requirements	service requirements	impl	derived	RRD:SG2.SP1 RRD:SG2.SP2

[41] May want to specifically categorize by source of realized risk that is of greatest interest such as incidents, control gaps, non-compliance, vulnerabilities, disruptions in continuity, etc.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
RRD-M3	percentage of assets with incomplete or no stated requirements	asset requirements	impl	derived	RRD:SG2.SP1 RRD:SG2.SP2
RRD-M4	percentage of service owners participating in the development of requirements (should be 100%)	service requirements	impl	derived	RRD:SG2.SP1 RRD:SG2.SP2
RRD-M5	percentage of asset owners participating in the development of requirements (should be 100%)	asset requirements	impl	derived	RRD:SG2.SP1 RRD:SG2.SP2
RRD-M6	percentage of documented requirements that have not been implemented[42]	enterprise, service, and asset requirements	impl; possibly effectiveness	derived	none
RRD-M7	percentage of assets for which the required level of functionality of the asset is not documented for all services it supports	asset requirements	impl	derived	RRD:SG3.SP1
RRD-M8	percentage of assets with requirements revisions due to: • conflicts resulting from associations with multiple services • requirements deficiencies • enterprise requirements • requirements gaps	asset requirements	impl	derived	RRD:SG3.SP2 RRD:SG3.SP3
RRD-M9	percentage of asset requirements conflicts for which mitigation plans have been developed but not implemented	asset requirements	impl	derived	RRD:SG3.SP2
RRD-M10	percentage of requirements that have not been analyzed to identify conflicts and interdependencies	asset requirements	impl	derived	RRD:SG3.SP2
RRD-M11	percentage of requirements whose adequacy has not been validated	asset requirements	impl	derived	RRD:SG3.SP3
RRD-M12	elapsed time between identification of new assets and the development of requirements for these assets (mean, median)	asset requirements	impl	base of type schedule	ADM:SG3.SP2 RRD:SG2.SP1
RRD-M13	costs of developing, analyzing, validating, documenting, and tracking requirements	enterprise, service, and asset requirements	impl	base of type cost	none
RRD-M14	percentage of service continuity test failures caused by incorrect or missing requirements	service requirements	effectiveness	derived	none
RRD-M15	percentage of incidents caused by incorrect or missing requirements	asset requirements	effectiveness	derived	none

Resilience Requirements Management (RRM)

The purpose of Resilience Requirements Management is to manage the resilience requirements of high-value services and associated assets and to identify inconsistencies between these requirements and the activities that the organization performs to meet the requirements.

Summary of Specific Goals and Practices

RRM:SG1 Manage Requirements

RRM:SG1.SP1 Obtain an Understanding of Resilience Requirements

[42] While included as an RRD measure of interest, implementation of requirements is covered in other PAs (enterprise – EF, RISK, etc.; service – EF, SC; asset – EC, KIM, PM, TM)

RRM:SG1.SP2 Obtain Commitment to Resilience Requirements

RRM:SG1.SP3 Manage Resilience Requirements Changes

RRM:SG1.SP4 Maintain Traceability of Resilience Requirements

RRM:SG1.SP5 Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
RRM-M1	percentage of assets for which agreement between asset owners and custodians on asset requirements has not been reached	asset requirements	impl	derived	RRM:SG1.SP1
RRM-M2	percentage of service level agreements between asset owners and custodians that are pending sign-off due to requirements issues	asset requirements	impl	derived	RRM:SG1.SP2
RRM-M3	percentage of asset custodians who accept responsibility for implementing requirements, if applicable	asset requirements	impl	derived	RRM:SG1.SP1 RRM:SG1.SP2
RRM-M4	percentage of documented, agreed-to requirements that have not been implemented[43] as scheduled	enterprise, service, and asset requirements	impl	derived	none
RRM-M5	percentage of asset owners participating in managing changes to requirements for the assets they own	changes to requirements	impl	derived	RRM:SG1.SP3 also EC, KIM, TM
RRM-M6	number of approved requirements changes: • by asset category or type • by asset • by service • by change trigger and criteria	changes to requirements	impl	base of type count	RRM:SG1.SP3
RRM-M7	number of unapproved requirements changes	changes to requirements	effectiveness	base of type count	RRM:SG1.SP3
RRM-M8	number of approved requirements changes that have not been communicated to asset custodians (via defined channels or SLAs)	changes to requirements	impl	base of type count	RRM:SG1.SP3
RRM-M9	percentage of requirements change requests whose disposition is pending beyond schedule	changes to requirements	impl	derived	RRM:SG1.SP3
RRM-M10	percentage of approved requirements changes whose implementation is pending beyond schedule	changes to requirements	impl	derived	RRM:SG1.SP3
RRM-M11	percentage of requirements changes that are not subject to the organization's change control process	changes to requirements	impl	derived	RRM:SG1.SP3
RRM-M12	costs of analyzing, managing, documenting, and tracking changes to requirements	changes to requirements	impl	base of type cost	FRM:SG2.SP2 RRM:SG1.SP3
RRM-M13	percentage of requirements that are not traced to a source or origination (documented in the asset profile)	requirements traceability	impl	derived	RRM:SG1.SP4

[43] While included as an RRM measure of interest, actual implementation of requirements is covered in other PAs (enterprise – EF, RISK, etc.; service – EF, SC; asset – EC, KIM, PM, TM)

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
RRM-M14	percentage of resilience activities that are not traced to a requirement	requirements traceability	impl	derived	RRM:SG1.SP4
RRM-M15	number of inconsistencies detected between requirements and the activities in place to satisfy the requirements	enterprise, service, and asset requirements	impl	base of type count	RRM:SG1.SP5
RRM-M16	number of corrective actions to align requirements and the activities required to satisfy them that are open beyond threshold (as scheduled)	enterprise, service, and asset requirements	impl	base of type count	RRM:SG1.SP5
RRM-M17	elapsed time between major updates to assets (such as being associated with a new service) and updates to the requirements for these assets (mean, median)	asset requirements	impl	base of type schedule	ADM:SG3.SP2 RRM:SG1.SP3

Resilient Technical Solution Engineering (RTSE)

The purpose of Resilient Technical Solution Engineering is to ensure that software and systems are developed to satisfy their resilience requirements.

Summary of Specific Goals and Practices

RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development

RTSE:SG1.SP1 Identify General Guidelines

RTSE:SG1.SP2 Identify Requirements Guidelines

RTSE:SG1.SP3 Identify Architecture and Design Guidelines

RTSE:SG1.SP4 Identify Implementation Guidelines

RTSE:SG1.SP5 Identify Assembly and Integration Guidelines

RTSE:SG2 Develop Resilient Technical Solution Development Plans

RTSE:SG2.SP1 Select and Tailor Guidelines

RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process

RTSE:SG3 Execute the Plan

RTSE:SG3.SP1 Monitor Execution of the Development Plan

RTSE:SG3.SP2 Release Resilient Technical Solutions into Production

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
RTSE-M1	percentage of software assets that have been developed without resilience guidelines, by guideline type: • general • requirements • architecture and design • implementation • assembly and integration	resilience guidelines for software development	impl; possibly effectiveness	derived	RTSE:SG2.SP1 Could also be mapped to each of the SG1 specific practices

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
RTSE-M2	percentage of software assets that have been acquired without consideration of resilience guidelines, by guideline type: • general • requirements • architecture and design • implementation • assembly and integration	resilience guidelines for software acquisition	impl; possibly effectiveness	derived	RTSE:SG2.SP1 Could also be mapped to each of the SG1 specific practices
RTSE-M3	percentage of software development staff trained in the tailoring and use of resilience guidelines, by guideline type: • general • requirements • architecture and design • implementation • assembly and integration	resilience guidelines for software development	impl; possibly effectiveness	derived	RTSE:SG2.SP1 Could also be mapped to each of the SG1 specific practices
RTSE-M4	life-cycle costs associated with implementing each resilience guideline (time, staff resources, and funding, including training) or some meaningful collection of guidelines	resilience guideline costs	impl	derived	RTSE:SG2.SP1 Could also be mapped to each of the SG1 specific practices
RTSE-M5	percentage of resilience requirements not satisfied by a specific software or system asset[44] ranked in priority order (refer to RRD) by life-cycle phase	resilience requirements	impl	derived	RTSE:SG3.SP1 RTSE:SG3.SP2
RTSE-M6	percentage of resilience requirements not satisfied by a specific software or system asset, where lack of satisfaction has been identified as a residual risk to be managed	resilience requirements; risk identification	impl	derived	RTSE:SG3.SP1 RTSE:SG3.SP2
RTSE-M7	number of defects and vulnerabilities above threshold for a specific software or system asset by life-cycle phase	vulnerabilities and defects	impl	base of type count	RTSE:SG3.SP1
RTSE-M8	number of defects and vulnerabilities above threshold for a specific software or system asset where such defects and vulnerabilities have documented mitigation plans	vulnerabilities and defects	impl	base of type count	RTSE:SG3.SP1
RTSE-M9	number of defects and vulnerabilities above threshold for a specific software or system asset where such defects and vulnerabilities have been identified as residual risks to be managed	vulnerabilities and defects; risk identification	impl	base of type count	RTSE:SG3.SP1
RTSE-M10	number of defects and vulnerabilities above threshold for a specific software or system assets where the presence of such defects and vulnerabilities is a result of not implementing a resilience guideline	vulnerabilities and defects	impl	base of type count	RTSE:SG3.SP1
RTSE-M11	percentage of software assets for which some form of risk assessment has not been performed and documented (per policy or other resilience guidelines) and within the specified time frame, by life-cycle phase	asset risk	impl	derived	RTSE:SG2.SP1 RTSE:SG2.SP2 RTSE:SG3.SP1

[44] This presumes that criteria for satisfaction are well established, such as evidence associated with one or more assurance cases or the results of specific review milestones or selected test cases.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
RTSE-M12	percentage of system assets for which some form of risk assessment has not been performed and documented (per policy or other resilience guidelines) and within the specified time frame, by life-cycle phase	asset risk	impl	derived	RTSE:SG2.SP1 RTSE:SG2.SP2 RTSE:SG3.SP1
RTSE-M13	number of unauthorized changes to software assets, by life-cycle phase	asset change management	impl	base of type count	RTSE:SG3.SP1
RTSE-M14	number of unauthorized changes to system assets, by life-cycle phase	asset change management	impl	base of type count	RTSE:SG3.SP1
RTSE-M15	inspection yield: defects found during the inspection / (defects found during the inspection + those that escaped the inspection)	inspections	effectiveness	derived	RTSE:SG3.SP2
RTSE-M16	inspection removal rate: effort spent in inspection / number of defects found in inspection	inspections	effectiveness	derived	RTSE:SG3.SP2
RTSE-M17	planned versus actual number of inspections	inspections	impl	derived	RTSE:SG3.SP2
RTSE-M18	percentage of software assets released into production without consideration of resilience guidelines	resilience guidelines for released software	impl; possibly effectiveness	derived	RTSE:SG3.SP2
RTSE-M19	percentage of system assets released into production without consideration of resilience guidelines	resilience guidelines for released software	impl; possibly effectiveness	derived	RTSE:SG3.SP2
RTSE-M20	elapsed time between the identification of a newly released software or system asset and its inclusion in the asset inventory	asset inventory	impl; possibly effectiveness	base of type schedule	ADM:SG1.SP1
RTSE-M21	number of software and system development risks referred to the risk management process	risk identification	impl	base of type count	RTSE:SG3.SP1
RTSE-M22	percentage of software and system development policies that are met	policy	impl	derived	none
RTSE-M23	test defect density (number of vulnerabilities found in test / size of software asset)	system test	impl	derived	RTSE.SG1.SP4
RTSE-M24	usage defect density (number of vulnerabilities found while using software or number of incidents that occurred while using software / size of software asset)	integration test; acceptance test; usage	impl	derived	RTSE.SG1.SP5

Service Continuity (SC)

The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

Summary of Specific Goals and Practices

SC:SG1 Prepare for Service Continuity

SC:SG1.SP1 Plan for Service Continuity

SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity

SC:SG2 Identify and Prioritize High-Value Services

SC:SG2.SP1 Identify the Organization's High-Value Services

SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies

SC:SG2.SP3 Identify Vital Organizational Records and Databases

SC:SG3 Develop Service Continuity Plans

SC:SG3.SP1 Identify Plans to Be Developed

SC:SG3.SP2 Develop and Document Service Continuity Plans

SC:SG3.SP3 Assign Staff to Service Continuity Plans

SC:SG3.SP4 Store and Secure Service Continuity Plans

SC:SG3.SP5 Develop Service Continuity Plan Training

SC:SG4 Validate Service Continuity Plans

SC:SG4.SP1 Validate Plans to Requirements and Standards

SC:SG4.SP2 Identify and Resolve Plan Conflicts

SC:SG5 Exercise Service Continuity Plans

SC:SG5.SP1 Develop Testing Program and Standards

SC:SG5.SP2 Develop and Document Test Plans

SC:SG5.SP3 Exercise Plans

SC:SG5.SP4 Evaluate Plan Test Results

SC:SG6 Execute Service Continuity Plans

SC:SG6.SP1 Execute Plans

SC:SG6.SP2 Measure the Effectiveness of the Plans in Operation

SC:SG7 Maintain Service Continuity Plans

SC:SG7.SP1 Establish Change Criteria

SC:SG7.SP2 Maintain Changes to Plans

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
SC-M1	elapsed time since the organization-wide plan for managing SC and the standards and guidelines for SC were reviewed and updated	SC program	impl	base of type schedule	SC:SG1.SP1 SC:SG1.SP2
SC-M2	percentage of unstaffed roles and responsibilities in the organization-wide plan for managing SC	SC program	impl	derived	SC:SG1.SP1
SC-M3	percentage of SC guidelines and standards that are more/less stringent than required to meet compliance obligations	SC program	impl	derived	SC:SG1.SP1 SC:SG1.SP2
SC-M4	number of relationships[45] (organization-wide, by SC plan) necessary to ensure SC	SC program	impl	base of type count	SC:SG2.SP2
SC-M5	number of points of contact for relationships that require updates	SC program	impl	base of type count	SC:SG2.SP2
SC-M6	elapsed time since review and update of the list of vital organizational records and databases	SC program	impl	base of type schedule	SC:SG2.SP3

[45] Internal dependencies, external dependencies, and interdependencies (refer to SC:SG2.SP2)

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
SC-M7	percentage of SC plans completed	SC plan development	impl	derived	SC:SG3.SP2
SC-M8	number of required SC plans that have not yet been developed (based on high-value services and associated assets that do not have SC plans)	SC plan development	impl	base of type count	SC:SG2.SP1 SC:SG3.SP1
SC-M9	percentage of SC plans that are not stored in a central storage system	SC plan development	impl	derived	SC:SG3.SP4
SC-M10	percentage of plans that are dependent on other plans; number of plans on which they are dependent	SC plan dependencies	impl	derived; base of type count	SC:SG4.SP2
SC-M11	percentage of plans with missing components (designated owner, resources, etc.)	SC plan omissions	impl	derived	SC:SG3.SP2
SC-M12	percentage of plans without established owners	SC plan omissions	impl	derived	SC:SG3.SP2
SC-M13	percentage of plans without identified stakeholders	SC plan omissions	impl	derived	SC:SG3.SP2
SC-M14	number of staff assigned to SC plans that are no longer employed by the organization	SC plan omissions	impl	base of type count	SC:SG3.SP3
SC-M1	percentage of defined roles in SC plans that are not assigned to specific staff	SC plan omissions	impl	derived	SC:SG3.SP3
SC-M15	percentage of defined roles in SC plans for which backup staff are not identified	SC plan omissions	impl	derived	SC:SG3.SP3
SC-M16	percentage of SC plans that do not meet service and asset resilience requirements	SC plan omissions	impl	derived	SC:SG4.SP1
SC-M17	percentage of SC plans that do not meet standards and guidelines	SC plan omissions	impl	derived	SC:SG4.SP1
SC-M18	percentage of staff not covered by a service continuity plan	SC plan omissions	impl	derived	none
SC-M19	percentage of staff who have not been trained on their roles and responsibilities as defined in SC plans	SC plan training	impl	derived	SC:SG3.SP5
SC-M20	percentage of plans with one or more severe conflicts (such as a single point of failure) that have not been mitigated	SC plan conflicts	impl	derived	SC:SG4.SP2
SC-M21	percentage of SC plans that do not have a schedule for testing and review	SC plan testing	impl	derived	SC:SG5.SP1
SC-M22	percentage of SC plans that do not have a test plan	SC plan testing	impl	derived	SC:SG5.SP2
SC-M23	percentage of SC test plans that have/have not been exercised	SC plan testing	impl	derived	SC:SG5.SP3
SC-M24	percentage of interdependent service continuity plans that have/have not been jointly tested	SC plan testing	impl	derived	SC:SG5.SP3
SC-M25	percentage of SC test plans that have failed one or more test objectives	SC plan testing	impl	derived	SC:SG5.SP4
SC-M26	percentage of SC plan test objectives (RTOs and RPOs) unmet	SC plan testing	impl	derived	SC:SG5.SP4
SC-M27	number of staff with defined roles in SC plans who do not have access to such plans within specified thresholds (time)	SC plan testing	impl	base of type count	SC:SG3.SP4
SC-M28	average time for staff with defined SC plan roles to access SC plans	SC plan testing	impl	base of type schedule	SC:SG3.SP4 SC:SG5.SP3

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
SC-M29	percentage of realized risks for service continuity that exceed established risk parameters	SC risk	effectiveness	derived	none
SC-M30	percentage of SC plans executed (never executed)	SC plan execution	impl	base of type count; derived	SC:SG6.SP1
SC-M31	percentage of plans that have not been reviewed post-execution	SC plan review	impl	derived	SC:SG6.SP2
SC-M32	percentage of plans that require changes (as defined by change criteria)	SC plan changes	impl	derived	SC:SG7.SP1 SC:SG7.SP2
SC-M33	percentage of plans that have been changed without authorization	SC plan changes	impl	derived	SC:SG7.SP2
SC-M34	percentage of plans that have been changed without review	SC plan changes	impl	derived	SC:SG7.SP2
SC-M35	percentage of plans that have been changed without testing	SC plan changes	impl	derived	SC:SG7.SP2
SC-M36	frequency of changes to plans by service or service type	SC plan changes	impl	base of type schedule	SC:SG7.SP2

Technology Management (TM)

The purpose of Technology Management is to establish and manage an appropriate level of controls related to the integrity and availability of technology assets to support the resilient operations of organizational services.

Summary of Specific Goals and Practices

TM:SG1 Establish and Prioritize Technology Assets

- TM:SG1.SP1 Prioritize Technology Assets
- TM:SG1.SP2 Establish Resilience-Focused Technology Assets

TM:SG2 Protect Technology Assets

- TM:SG2.SP1 Assign Resilience Requirements to Technology Assets
- TM:SG2.SP2 Establish and Implement Controls

TM:SG3 Manage Technology Asset Risk

- TM:SG3.SP1 Identify and Assess Technology Asset Risk
- TM:SG3.SP2 Mitigate Technology Risk

TM:SG4 Manage Technology Asset Integrity

- TM:SG4.SP1 Control Access to Technology Assets
- TM:SG4.SP2 Perform Configuration Management
- TM:SG4.SP3 Perform Change Control and Management
- TM:SG4.SP4 Perform Release Management

TM:SG5 Manage Technology Asset Availability

- TM:SG5.SP1 Perform Planning to Sustain Technology Assets
- TM:SG5.SP2 Manage Technology Asset Maintenance
- TM:SG5.SP3 Manage Technology Capacity

TM:SG5.SP4 Manage Technology Interoperability

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
TM-M1	percentage of technology assets that have been inventoried	asset inventory	impl	derived	ADM SG1.SP1
TM-M2	percentage of technology assets with/without a complete asset profile (such as no stated resilience requirements)	asset inventory	impl	derived	ADM:SG1.SP2 TM:SG2.SP1
TM-M3	percentage of technology assets with/without a designated owner	asset inventory	impl	derived	ADM:SG1.SP3
TM-M4	percentage of technology assets with/without a designated custodian	asset inventory	impl	derived	ADM:SG1.SP3
TM-M5	percentage of technology assets that have designated owners but no custodians	asset inventory	impl	derived	ADM:SG1.SP3
TM-M6	percentage of technology assets that have designated custodians but no owners	asset inventory	impl	derived	ADM:SG1.SP3
TM-M7	percentage of technology assets that have been inventoried, by service	asset inventory	impl	derived	ADM:SG2.SP1
TM-M8	percentage of technology assets that are not associated with one or more services	asset inventory	impl	derived	ADM:SG2.SP1
TM-M9	percentage of technology asset-service dependency conflicts with unimplemented or incomplete mitigation plans	asset-service dependencies	impl	derived	ADM:SG2.SP2
TM-M10	percentage of technology asset-service dependency conflicts with no mitigation plans	asset-service dependencies	impl	derived	ADM:SG2.SP2 TM:SG2.SP2
TM-M11	number of discrepancies between the current inventory and the previous inventory	asset inventory	impl	base of type count	ADM SG3.SP1
TM-M12	number of changes made to asset profiles in the technology asset inventory	asset inventory	impl	base of type count	ADM SG3.SP2
TM-M13	number of changes to resilience requirements as a result of technology asset changes	asset change management	impl	base of type count	ADM:SG3.SP2
TM-M14	number of changes to service continuity plans as a result of technology asset changes	asset change management	impl	base of type count	ADM:SG3.SP2
TM-M15	percentage of technology assets that are designated as high-value assets	asset inventory	impl	derived	TM:SG1.SP1
TM-M16	elapsed time since the technology asset inventory was last reviewed	asset inventory	impl	base of type schedule	ADM:SG1.SP1 ADM:SG3.SP1
TM-M17	elapsed time since review and validation of high-value technology assets and their priorities	asset inventory	impl	base of type schedule	TM:SG1.SP1
TM-M18	elapsed time since review and reconciliation of resilience-focused technology assets (those required for service continuity & service restoration)	asset inventory	impl	base of type schedule	TM:SG1.SP2

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
TM-M19	percentage of technology assets without assigned/defined resilience requirements	asset requirements	impl	derived	TM:SG2.SP1
TM-M20	percentage of technology assets with assigned/defined resilience requirements that are undocumented	asset requirements	impl	derived	TM:SG2.SP1
TM-M21	percentage of technology assets that do not satisfy their resilience requirements	asset requirement	impl	derived	TM:SG2.SP1
TM-M22	percentage of technology assets with no or missing protection controls	asset controls	impl; possibly effectiveness	derived	TM:SG2.SP2
TM-M23	percentage of technology assets with no or missing sustainment controls	asset controls	impl; possibly effectiveness	derived	TM:SG2.SP2
TM-M24	percentage of technology asset controls (protection and sustainment) that are ineffective or inadequate as demonstrated by: • unsatisfied control objectives • unmet resilience requirements • outstanding control assessment problem areas above established thresholds and without remediation plans	asset controls	impl; possibly effectiveness	derived	TM:SG2.SP2
TM-M25	percentage of technology asset control deficiencies not resolved by scheduled due date (refer to CTRL measures for categories of control deficiencies)	asset controls	impl	derived	TM:SG2.SP2
TM-M26	elapsed time since review of the effectiveness of technology asset controls	asset controls	impl	base of type schedule	TM:SG2.SP2
TM-M27	elapsed time since risk assessment of technology assets performed	asset risk	impl	base of type schedule	TM:SG3.SP1
TM-M28	elapsed time since business impact analysis of technology assets performed	asset risk	impl	base of type schedule	TM:SG3.SP1
TM-M29	percentage of technology assets for which business impact valuation[46] has not been performed	asset risk	impl	derived	TM:SG3.SP1
TM-M30	percentage of technology assets for which a risk assessment has not been performed and documented (per policy or other guideline) and according to plan	asset risk	impl	derived	TM:SG3.SP1 TM:SG5.SP4 subpractice 3
TM-M31	percentage of technology asset risks that have not been assigned to a responsible party for action, tracking, and closure	asset risk	impl	derived	TM:SG3.SP2
TM-M32	percentage of technology asset risks[47] with a disposition of “mitigate or control” that do not have a defined mitigation plan	asset risk	impl	derived	TM:SG3.SP2[48]

[46] Business impact valuation can be either qualitative (high, medium, low) or quantitative (based on levels of loss or damage, fines, number of customers lost, disruption in access, etc.)

[47] This measure also appears in RISK M4-1. For ease of use of an individual PA (vs. ease of maintenance and consistency), we have decided to replicate some (but not all) risk-related measures in the individual asset PAs that are identified generally in the list of RISK PA measures.

[48] SG3.SP2 subpractice 7 states, “Collect performance measures on the risk management process.” No such measures are included here in TM; refer to the RISK PA.

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
TM-M33	percentage of technology asset risks with a "mitigate or control" disposition that are not effectively mitigated by their mitigation plans	asset risk	effec-tiveness	derived	TM:SG3.SP2
TM-M34	percentage of realized risks for technology assets that exceed established risk parame-ters	asset risk	effec-tiveness	derived	TM:SG3.SP2
TM-M35	number of violations of access control policies for technology assets	asset access controls	impl	base of type count	TM:SG4.SP1
TM-M36	percentage of intrusions into digital technology assets where impact exceeds threshold	asset intrusions	impl	derived	TM:SG4.SP1
TM-M37	percentage of intrusions into physical technol-ogy assets where impact exceeds threshold	asset intrusions	impl	derived	TM:SG4.SP1
TM-M38	elapsed time since audit of technology asset modification logs	asset access controls	impl	base of type schedule	TM:SG4.SP1
TM-M39	percentage of technology assets for which approved configuration settings have/have not been implemented as required by policy	asset configu-ration	impl	derived	TM:SG4.SP2
TM-M40	percentage of technology assets with configu-rations that deviate from approved standards for which exceptions have not been granted	asset configu-ration	impl	derived	TM:SG4.SP2
TM-M41	elapsed time since review of technology asset configuration control logs	asset configu-ration	impl	base of type schedule	TM:SG4.SP2
TM-M42	elapsed time since audit of technology asset configurations	asset configu-ration	impl	base of type schedule	TM:SG4.SP2
TM-M43	number of unauthorized changes to technolo-gy assets (may need to report by some mea-ningful categorization of assets)	asset change management	impl	base of type count	TM:SG4.SP3
TM-M44	change success rate (percentage of changes to technology assets that succeed without causing an incident, service outage, or im-pairment)	asset change management	impl	derived	TM:SG4.SP3
TM-M45	percentage of changes that are high-priority, emergency changes	asset change management	impl	derived	TM:SG4.SP3
TM-M46	percentage of changes that result from defi-ciencies in resilience requirements	asst change management	impl	derived	TM:SG4.SP3
TM-M47	elapsed time between: • scheduled technology asset configuration updates and actual configuration updates • scheduled technology asset changes and actual changes • scheduled technology asset releases into production and actual releases	asset configu-ration, change, and release management	impl	base of type schedule	TM:SG4.SP2 TM:SG4.SP3 TM:SG4.SP4
TM-M48	percentage of technology assets approved for release into production that have not under-gone a security review	asset release management	impl	derived	TM:SG4.SP4
TM-M49	percentage of technology assets released into production that have not undergone security testing in accordance with policy	asset release management	impl	derived	TM:SG4.SP4
TM-M50	percentage of technology assets released to production that deviate from approved stan-dards for which exceptions have not been granted	asset release management	impl	derived	TM:SG4.SP4

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
TM-M51	percentage of technology assets without availability metrics	asset sustainment	impl	derived	TM:SG5.SP1
TM-M52	percentage of technology assets without recovery time objectives (RTO)	asset sustainment	impl	derived	TM:SG5.SP1
TM-M53	percentage of technology assets without recovery point objectives (RPO)	asset sustainment	impl	derived	TM:SG5.SP1
TM-M54	number of technology assets that do not have their own service continuity plan where one is required	asset sustainment	impl	base of type count	TM:SG5.SP1
TM-M55	percentage of external entities that are not meeting service level agreements for technology assets subject to external entity services	asset sustainment	impl	derived	none
TM-M56	elapsed time since technology asset maintenance performed	asset maintenance	impl	base of type schedule	TM:SG5.SP2
TM-M57	number of scheduled maintenance activities that exceed recommended service intervals	asset maintenance	impl	base of type count	TM:SG5.SP2
TM-M58	number of scheduled maintenance activities that do not meet recommended specifications	asset maintenance	impl	base of type count	TM:SG5.SP2
TM-M59	number of maintenance changes that were made without following change management procedures	asset maintenance	impl	base of type count	TM:SG5.SP2
TM-M60	number of technology assets requiring capacity management for which no forecast or strategy exists	asset capacity	impl	base of type count	TM:SG5.SP3
TM-M61	elapsed time since the capacity management strategy for technology assets has been validated and updated	asset capacity	impl	base of type schedule	TM:SG5.SP3
TM-M62	elapsed time since the technology asset interoperability strategy has been reviewed	asset capacity	impl	base of type schedule	TM:SG5.SP4

Vulnerability Analysis and Resolution (VAR)

The purpose of Vulnerability Analysis and Resolution is to identify, analyze, and manage vulnerabilities in an organization's operating environment.

Summary of Specific Goals and Practices

VAR:SG1 Prepare for Vulnerability Analysis and Resolution

VAR:SG1.SP1 Establish Scope

VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy

VAR:SG2 Identify and Analyze Vulnerabilities

VAR:SG2.SP1 Identify Sources of Vulnerability Information

VAR:SG2.SP2 Discover Vulnerabilities

VAR:SG2.SP3 Analyze Vulnerabilities

VAR:SG3 Manage Exposure to Vulnerabilities

VAR:SG3.SP1 Manage Exposure to Vulnerabilities

VAR:SG4 Identify Root Causes

VAR:SG4.SP1 Perform Root-Cause Analysis

Measures

ID	Measure	Type of Information	Measure Type	Base or Derived	Applicable SG.SP
VAR-M1	percentage of high-value assets (by type or category) subject to VAR process activities (This is determined by the resilience requirements associated with assets and assumes an up-to-date asset inventory *[refer to ADM]*.)	asset inventory; ORMS scope	impl	derived	ADM:SG1.SP1 ADM:SG1.SP2
VAR-M2	percentage of high-value assets that have been monitored for vulnerabilities within an agreed-upon time interval	vul monitoring	impl	derived	ADM:SG1.SP1 MON:SG2.SP3
VAR-M3	percentage of high-value assets that have been audited or assessed for vulnerabilities	vul assessment	impl	derived	ADM:SG1.SP1 VAR:SG2.SP2
VAR-M4	percentage of reported vulnerabilities (by asset type or category) that require some form of resolution or remediation (course of action, reduction, elimination)	vul resolution	impl	derived	VAR:SG2.SP3
VAR-M5	percentage of vulnerabilities that have been satisfactorily remediated	vul resolution	effectiveness	derived	VAR:SG3.SP1
VAR-M6	percentage of open vulnerabilities	vul resolution	impl	derived	VAR:SG3.SP1
VAR-M7	percentage of vulnerabilities that require resolution for which a vulnerability management strategy exists	vul resolution	impl	derived	VAR:SG3.SP1
VAR-M8	percentage of vulnerabilities with vulnerability management strategies that are on track per plan	vul resolution	impl	derived	VAR:SG3.SP1
VAR-M9	percentage of vulnerabilities requiring a root-cause analysis	vul analysis	impl	derived	VAR:SG4.SP1
VAR-M10	number of vulnerabilities that result in incidents for which a root-cause analysis was not performed	vul analysis	impl	base of type count	VAR:SG4.SP1
VAR-M11	number of vulnerabilities referred to the incident management and control process	incident analysis	impl	base of type count	none
VAR-M12	number of vulnerabilities referred to the service continuity process	SC requirements	impl	base of type count	none
VAR-M13	elapsed time from high-value vulnerability data collection to data distribution to key stakeholders	vul communication	effectiveness	base of type schedule	VAR:GG2.GP7
VAR-M14	number of vulnerabilities referred to the risk management process	risk identification	impl	base of type count	VAR:SG2.SP3
VAR-M15	percentage of organizational units, lines of business, and services using vulnerability data to assess the performance of operational resilience management processes	ORMS assessment	process performance	derived	none

References

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

[Allen 2010]
Allen, Julia & Davis, Noopur. *Measuring Operational Resilience Using the CERT Resilience Management Model* (CMU/SEI-2010-TN-030). Software Engineering Institute, Carnegie Mellon University, September 2010.
http://www.sei.cmu.edu/library/abstracts/reports/10tn030.cfm

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

[Caralli 2011]
Caralli, Richard A.; Allen, Julia H.; & White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Measures for Managing Operational Resilience	FA8721-05-C-0003

6. AUTHOR(S)

Julia H. Allen, Pamela D. Curtis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2011-TR-019

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-2011-019

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

How resilient is my organization? Have our processes made us more resilient? Members of the CERT® Resilient Enterprise Management (REM) team are conducting research to address these and other related questions. The team's first report, Measuring Operational Resilience Using the CERT Resilience Management Model, defined high-level objectives for managing an operational resilience management (ORM) system, demonstrated how to derive meaningful measures from those objectives, and presented a template for defining resilience measures, along with example measures.

In this report, REM team members suggest a set of top ten strategic measures for managing operational resilience. These measures derive from high-level objectives of the ORM system defined in the CERT® Resilience Management Model, Version 1.1 (CERT®-RMM). The report also provides measures for each of the 26 process areas of CERT-RMM, as well as a set of global measures that apply to all process areas. This report thus serves as an addendum to CERT-RMM Version 1.1.

Since CERT-RMM practices map to bodies of knowledge and codes of practice such as ITIL, COBIT, ISO2700x, BS25999, and PCI DSS, the measures may be useful for measuring security, business continuity, and IT operations management processes, either as part of adoption of CERT-RMM or independent of it.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Resilience management, risk, measure, measurement, enterprise security management, strategic planning, information security, risk management, operational risk management, process improvement, resilience, operational resilience, CERT-RMM	81

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