Software Engineering Institute

Using Defined Processes as a Context for Resilience Measures

Julia H. Allen
Pamela D. Curtis
Linda Parker Gates

December 2011

TECHNICAL NOTE
CMU/SEI-2011-TN-029

CERT® Program

http://www.sei.cmu.edu

Carnegie Mellon

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

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

This report was prepared for the

SEI Administrative Agent
ESC/CAA
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

* These restrictions do not apply to U.S. government entities.

Table of Contents

Acknowledgments **iii**

Abstract **v**

1 Introduction **1**

1.1 Why Define Processes? 1

1.2 Why Use Defined Processes as a Basis for Selecting and Defining Measures? 2

2 Defining Processes and Procedures **3**

2.1 Process Definition Elements 3

2.2 Defining Processes 3

2.3 Defining Procedures 4

3 Selecting Measures **5**

3.1 Defining Measures 6

4 Future Plans **7**

Appendix A: Process Definition Example and Template **9**

Appendix B: Procedure Definition Example and Template **19**

Appendix C: Information Asset Profile Example and Template **27**

Appendix D: Alternative Process or Procedure Example and Template **35**

Appendix E: Measure Definition Example and Template **41**

References **46**

Acknowledgments

The authors would like to thank the reviewers of this report who generously contributed their time, knowledge, and experience to provide comments that greatly enhanced the clarity and accuracy of the concepts presented. Reviewers are members of the CERT® Resilient Enterprise Management team, the CERT Enterprise and Workforce Development team, and the Software Engineering Institute’s Software Engineering Process Management program:

- Richard Barbour
- James Cebula
- Lisa Marino
- Michael Rattigan
- Barbara Tyson
- David White
- Lisa Young

The authors would also like to thank the members of the CERT® Resilience Management Model (CERT®-RMM) Users Group, who are using these materials and providing feedback as part of their organizational improvement projects.

Abstract

The CERT® Resilient Enterprise Management (REM) team is researching operational resilience and the organizational processes that support it. This technical note, which builds on two previous reports, describes how implementation-level processes can provide the necessary context for identifying and defining measures of operational resilience. The team's first report, *Measuring Operational Resilience Using the CERT® Resilience Management Model* (CMU/SEI-2010-TN-030), defined high-level objectives for an operational resilience management system, demonstrated how to derive meaningful measures from those objectives, and presented a template for defining resilience measures. The team's second report, *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019), suggested strategic measures for managing operational resilience and provided candidate measures for the 26 process areas of the CERT® Resilience Management Model, Version 1.1 (CERT®-RMM).

While CERT-RMM defines the commonly used or best practices for operational resilience—*what* an organization should do—organization-specific processes must be defined at the implementation level to describe *how* to perform those practices. Organizations can then identify and define measures within the context of their specific processes and procedures. Organizations can use the measures to evaluate process performance and operational resilience and identify opportunities for improvement. This technical note provides examples and templates for defining processes and procedures and for defining related assets and measures.

1 Introduction

In January 2010, the CERT[®] Program initiated the resilience measurement and analysis research project. This technical note is the third in a series describing an approach for measuring operational resilience using the CERT[®] Resilience Management Model (CERT[®]-RMM) as the reference maturity model. Readers are encouraged to read *Measuring Operational Resilience Using the CERT[®] Resilience Management Model* [Allen 2010] and *Measures for Managing Operational Resilience* [Allen 2011], the first two reports in this series, for the background and foundation for this technical note.

1.1 Why Define Processes?

A process definition describes the activities and tasks necessary to perform work consistently. Defined processes allow for repeatability and prediction and also form a foundation for measurement and improvement of operational resilience. In fact, a key prerequisite for identifying appropriate process measures is a defined and well-understood process.

Process measures are integral to resilience improvement because they make it possible to predict the impact of proposed changes and assess their results. Process measures can also help demonstrate that investments in operational resilience have measurable business value. Having clear process improvement goals will determine the kinds of entities and attributes that must be measured.

There is a cost associated with defining processes and keeping process definitions up to date. It is not always possible or necessary to define every process an organization enacts. It is, however, necessary to define processes if an organization wishes to analyze, measure, or improve them. In fact, defined processes facilitate a number of organizational objectives:

- facilitating feedback and learning
- providing a basis for improvement
- simplifying the execution of routine tasks
- making work manageable and predictable (and thus more easily planned)
- ensuring consistent, high-quality implementation (which can assist with high-risk or externally regulated processes)
- reducing the need for reinvention

A maturity model such as CERT-RMM defines commonly used or best practices—*what* an organization should do. But maturity models are not measurable. Process definitions describe *how* an organization actually performs work and are specific to organizations, people, facilities, and operations. A well-understood, well-defined, implemented process is a prerequisite for measurement of operational resilience; a maturity model cannot satisfy this need.

CERT-RMM guides both assessment and improvement of operational resilience processes. Defining (and refining) a process in the context of a maturity model, coupled with measurement, is a powerful tool for improvement.

[®] CERT, CERT Resilience Management Model, and CERT-RMM are registered marks owned by Carnegie Mellon University.

1.2 Why Use Defined Processes as a Basis for Selecting and Defining Measures?

Measurement supports transforming strategic direction, policy, and other forms of management decisions into action and evaluating the performance of such action. The right measures express:

- the extent to which objectives are being met
- how well requirements are being satisfied
- how well processes and controls are functioning
- the extent to which performance outcomes are being achieved

The CERT resilience measurement and analysis research project is focused on examining *what* should be measured to determine whether process performance objectives for operational resilience are being achieved and *how* performance should be measured. While measuring operational resilience may be most accurately done during or after times of stress and disruption, this is often too late to be beneficial. Typically, the organization is in too reactive a mode even to consider how to improve in anticipation of the next incident. Also, knowing how well the organization responded to previous attacks is not sufficient. The organization must be able to predict how it will perform in the future when the threat and risk environment changes.

An organization may gain more confidence and precision about its state of readiness by examining the fidelity and performance of the *processes* that contribute to its operational resilience—these are, at least, two important indicators that are not typically measured today. Such an examination requires defining and improving processes at the implementation level, as described in Section 1.1, and then identifying and defining measures within the context of these processes and their corresponding procedures. The intent is to collect, analyze, and report in-process measures as processes are being performed and use such measures to evaluate process performance, identify process improvements, and better understand the organization's capability to manage operational resilience. In addition, defined processes support and enable the consistent measurement of activities that may be outside the scope of evaluating process performance. For example, if an organization has a defined process for managing incidents, then it should have much more confidence in measures related to the number of incidents and their impact over time. If an organization instead performs ad hoc incident management, the number of incidents counted could be suspect. Defined processes produce related measures that are more collectible, consistent, reliable, and accurate.

To make informed decisions, affect behavior, and manage any activity, including operational resilience, organizational leaders need consistent, timely, and accurate measurements. A quotation often attributed to Deming states, "If you can't describe what you are doing as a process, you don't know what you're doing."[1] And if you don't know what you are doing, measurement and analysis will not help. Attempting to measure operational resilience without the foundation of a defined process is not very meaningful.

In the following sections, we describe an approach for defining processes and their corresponding procedures, and then selecting and defining measures based on those processes.

[1] "W. Edwards Deming." BrainyQuote.com. Xplore Inc, 2010. Accessed September 22, 2011. http://www.brainyquote.com/quotes/quotes/w/wedwardsd133510.html

2 Defining Processes and Procedures[2]

2.1 Process Definition Elements

A process is a systematic series of actions directed to some end.[3] The building blocks of process definitions are activities, people, and work products (also known as activities, agents, and artifacts). A process definition describes the work product or result of the process, the activities that produce that result and their sequence, and the roles that individuals or teams play in achieving the outcome—in essence, what happens, who does it, and what is accomplished. There are several other elements that make up a thorough definition of a process, as shown in Table 1.

Table 1: Key Process Definition Elements

Process Definition Element	Description
Purpose	The reason for performing the process
Scope	The extent or range of the process
Activities	The specific actions that are taken
Process Flow Diagram	A graphical depiction of the layout of the process activities
Inputs	Work products necessary for executing the process
Outputs	Work products generated by the process
Entry Criteria	Conditions that must be met for the process to begin
Exit Criteria	Conditions that must be met for the process to be considered complete
Roles	The functions people serve in the process
Requirements	Any demands placed on the process by the organization or type of work, and any resilience requirements that apply to the people, information assets, technology assets, and facilities involved in the process[4]
Controls	Policies, standards, or methods that limit the process or help satisfy process requirements
Mechanisms	Tools or systems used to assist the process
Verification	Activities to verify the consistent use of the process
Measures	Activities to assess process performance and to collect and analyze information needed to evaluate the extent to which management objectives are being met

2.2 Defining Processes

There are many tools and techniques available for defining processes (see, for example, Humphrey [1989] and SPC [1996]). The Total Quality Management (TQM) literature, for example, provides many respected techniques, templates, and tools (see, for example, Brassard [2010]).

A quick and effective approach to documenting a process is to prepare an initial draft and then conduct an interview with a knowledgeable process user to verify and populate the draft. The draft is an assumptive view of how a process works, presented as a rough model. Although the draft may not accurately represent the way

[2] The process definition information in this section is based on material presented in the Software Engineering Institute's Mastering Process Improvement training course (http://www.sei.cmu.edu/training/p15b.cfm).

[3] "process" Dictionary.com. Accessed September 22, 2011. http://dictionary.reference.com/browse/process

[4] Appendix B provides a template for documenting resilience requirements for assets used in operational resilience processes.

the process actually works, it will help scope and jumpstart the interview. It allows quick alignment and shared understanding between the interviewer and the interviewee, who can then validate the high-level definition and provide details on the specific activities.

The set of key questions shown in Table 2 can be used to conduct a process definition interview.

Table 2: Key Questions for Defining a Process

Key Question	Process Definition Element
Why is the process performed?	Purpose
What is the scope of the process?	Scope
What work product(s) or results are generated by the process?	Outputs
What conditions must be met for the process to begin and end?	Entry and Exit Criteria
What work product(s) are required to initiate the process?	Inputs
What activities are performed and in what sequence?	Activities
Who performs the activities of the process?	Roles
What organizational, resilience, or other requirements apply to the process?	Requirements
What controls are used to satisfy the requirements?	Controls
What mechanisms are used to aid in the implementation of the process?	Mechanisms
What activities are performed to verify the consistent use of the process?	Verification
How is performance of the process assessed?	Measures

A process definition, usually a combination of graphics and text, facilitates analysis and execution of the process. As a model of a process, the process definition is not exhaustive, but it does define the activities, conditions, and other required context within which measurement is performed.

Appendix A provides an example process definition, “Data Handling,” and a process definition template. The template contains all the necessary elements for defining a process and using it as the context for measurement and improvement. Some of the elements will not be needed for certain processes. For example, a process might not have any externally imposed requirements. However, all elements in the template should be considered before determining that they are not needed.

2.3 Defining Procedures

As stated in Section 1.1, a process describes *how* an organization actually performs work and is specific to organizations, people, facilities, and operations. But a process is not always fully implementable if it is not specified at the level of detail required to perform the process. In fact, it is often desirable to have a general-purpose process that can be applied to a broad range of activities or work products. A procedure, then, provides detailed instructions, often at the level of a particular activity, work product, or role, when more specificity is required to perform (and measure) the process. Appendix A defines an example data handling process that can be applied to a range of data types, and Appendix B defines an example procedure for a specific type of data.

Procedure definitions comprise the same kinds of elements that describe a process. Appendix B provides a procedure definition example and a procedure definition template. As with the process definition template, the procedure definition template contains all the necessary elements for defining a procedure as the context for measurement and improvement. Some of the elements will not be needed for certain procedures, but organizations should consider all elements in the template.

3 Selecting Measures

As described by Allen [2010], before an organization can select a measure, it must determine key information and context, including

- the resilience objective that the measure is intended to address. The objective should be connected to organizational strategic goals and critical success factors, organizational resilience goals, service resilience goals, and/or asset resilience goals. For example, a resilience objective might be “The Operational Resilience Management System (ORMS) manages (identifies, analyzes, mitigates) operational risks to high-value assets that could adversely affect the operation and delivery of high-value services,” and, more specifically, “Protect and sustain designated data.”
- the question(s) that the measure is intended to answer. For example, a question might be “How many incidents occurred during the last quarter?” or, more specifically, “How many breaches of confidentiality and privacy occurred as a result of unauthorized access of designated data in the last month?” The question should relate to the objective and to the defined processes that support the objective.

In this technical note, we add the process dimension to the set of key information by describing the related processes and procedures within which the measure is collected, analyzed, and reported.

The thought process and steps for selecting the 10 measures that are included in the Data Handling process example in Appendix A are described below. Based on our experience to date, we believe these steps (or some variation thereof) can be used to identify measures for any process. (The measure IDs are from the Measures table in the example.)

1. For the process overall or for each process activity, are there key stakeholder requirements that need to be satisfied? How would satisfaction be demonstrated? For example:
   a. A report reflecting the results of a survey or assessment must be received within 45 calendar days. One measure is “elapsed time between creation or receipt of data and delivery of data final report (mean, median)” (measure DH-M1).
   b. All designated data in digital form can only be accessed by those with a need to know. One measure is “number of breaches of confidentiality and privacy of designated data traced to violations of access control policies” (measure DH-M2; refer also to Appendix E for a complete definition of this measure).
   c. All data handling requirements are met. One measure is “number of violations of Data Handling requirements” (measure DH-M3).
2. For each process verification activity, what needs to be demonstrated to verify that the process was performed as defined and as expected? For example:
   a. Designated data that resides on access-controlled servers can be recovered and restored in accordance with service level agreements. One measure is “elapsed time (from initial request) to recover data from backups (mean, median)” (measure DH-M9).
3. Are there CERT-RMM v1.1 measures (as updated by Allen [2011]) that aid in determining the extent to which this process has been implemented? And the extent to which this process is effective? For example:

    a. difference in planned versus actual schedule (number of days) to perform the Data Handling process (measure DH-M4)
    b. difference in planned versus actual cost to perform the Data Handling process (measure DH-M5)

4. Evaluate what would need to be measured to determine if each process activity was performed as expected. For example:
    a. For the process activity “Create or receive the data,” one measure is “number of instances of data received or created” (measure DH-M4).
    b. For the process activity “Return or destroy the data,” one measure is “number of instances of data returned or destroyed” (measure DH-M7).
    c. For each data engagement, the two measures above would need to be compared and reconciled to ensure that all data received or created has been returned or destroyed, or that the designated party has explicitly approved retention of certain data (measure DH-M8).

Our intent is for each of these steps to demonstrate the value of having a defined process to use as the context for selecting measures. Without some defined process as the context, it is difficult to envision how meaningful measures would be selected and analyzed, how data to support such measures could be consistently collected, and how decisions and behavior would be informed by measurement reports. That said, in the absence of a defined process, resilience objectives and questions could be used as a starting point.

3.1 Defining Measures

Allen [2010] describes how using a measurement template helps thoroughly define a measure, including such information as who will use the measure, what is being measured, what data needs to be collected and where it is stored, how the data is collected, and how the measure is visually presented. Defining a measure using a template provides repeatability in collecting, analyzing, and reporting it. Appendix E shows an example of how a measure can be fully defined using the measurement template that was originally published in Allen [2010], updated to include traceability to related processes and procedures. The example uses measure DH-M2 from the Data Handling process.

4 Future Plans

This research project will continue through FY12 (October 2011 through September 2012). Future plans include the following:

- Assist in developing new process and procedure definitions as informed by selected customers and the CERT-RMM Users Group.[5]
- Pilot and improve selected implementation and effectiveness measures within the context of defined processes. Effectiveness measures, in particular, will be analyzed to determine the extent to which an improved process measurably contributes to improved operational resilience.
- Reflect new and updated measures in CERT-RMM v2.0.

The team will also develop additional measures templates for key measures (refer to Allen [2011] and Appendix E).

[5] For more information about the CERT-RMM Users Group, see http://www.sei.cmu.edu/training/P92.cfm.

Appendix A: Process Definition Example and Template

EXAMPLE

This fictitious example is a process for handling data submitted to or generated by ABC Organization.

Data Handling Process Definition

Process Purpose

The purpose of the Data Handling process is to protect and sustain designated data in accordance with ABC Organization requirements, compliance obligations, and policies and standard practices.

Scope

This process applies to designated data handled by ABC Organization staff.

Acronyms and Definitions

CERT®-RMM	CERT® Resilience Management Model

Outputs

- Resilient (protected and sustained) data as defined by CERT-RMM

Entry Criteria

- Data is created[6] or received.

Inputs

- Designated data that ABC Organization staff collect and develop:
    - survey data
    - diagnostic data
    - performance data
- Data that external parties provide and ABC Organization staff retain (documents, reports, spreadsheets, etc.)

Requirements

- Refer to the data set's information asset profile [see Appendix C for an example].

[6] Data creation begins the moment data is recorded or shared in physical form or digital form.

Controls

Policies

- ABC Organization Intellectual Property Policy

Procedures

- Survey Data Handling procedure
- Diagnostic Data Handling procedure
- Performance Data Handling procedure
- External Party Data Handling procedure

Standards

- ABC Organization Standard Practice for Dealing with the Media
- ABC Organization Standard Practice for Disclosure of Unclassified Information
- ABC Organization Controlled Information Management System Standard of Conduct and Procedures

Methods and Technologies

- ABC Organization Controlled Information Management System
- encrypted desktop and laptop hard drives
- encrypted WinZip files (for attachment to emails)
- access-controlled Microsoft SharePoint sites
- locked file cabinets

Mechanisms

Templates

- Survey report template
- Diagnostic report template
- Performance report template

Tools

- Microsoft SharePoint
- Disk encryption and decryption software
- WinZip-compatible encryption and decryption software

Roles

The following roles apply to the handling of designated data types:

Role	**Description**	**Responsibility**
ABC staff (exact role varies)	Staff member who participates in the receipt of data, has access to it, and handles it	In most cases, acts as a custodian of the data
ABC team/project lead	Leader of the team or project that conducts activities that handle data	Manages the conduct, reporting, and measurement associated with data handling activities
ABC editor	Technical editor	Edits reports containing the data
ABC IT administrator	IT staff member who backs up and restores data residing on SharePoint servers	Performs regular backups and tests ability to restore from backups; ensures that data that resides on SharePoint servers is encrypted

Activities

The following activities apply to the handling of designated data types unless otherwise noted in the applicable procedure for that data type:

Activity No.	Data Handling Activities	Description	Applicable Measures[a]	Role
1.0	Create or receive the data	Data is received or created in physical or digital form.	M1, M3, M4, M6, M8	ABC staff
2.0	Transport the data	Physical data is securely transported from one location to another, typically from the external party or other ABC site to the designated ABC site.	M2, M3	ABC staff
3.0	Store the data	Physical data is secured in safes or locked file cabinets. Digital data is encrypted on desktops and laptops. Digital data does not reside on mobile devices or removable storage devices. Digital data is stored on access-controlled SharePoint sites.	M2, M3	ABC team lead ABC staff
4.0	Share and access the data (internal to ABC Organization)	Digital data is accessed from access-controlled SharePoint sites. Digital data is encrypted and exchanged via email.	M2, M3	ABC team lead ABC staff ABC editor
5.0	Deliver the data (to an external party)	Digital data (e.g., reports, presentations) is encrypted and exchanged with an external party via email.	M1, M2, M3	ABC team lead ABC staff
6.0	Destroy or return the data	Physical and digital data is destroyed or returned in accordance with requirements.	M2, M3, M4, M7, M8	ABC team lead ABC staff
7.0	Back up the data	Digital data is backed up by ABC IT in accordance with the posted service level agreement. All backups are encrypted.		ABC IT administrator
8.0	Restore the data from backups	Upon ABC team lead request, data is restored to access-controlled SharePoint sites as needed. The ability to restore digital data from backups is regularly tested in accordance with the posted service level agreement.	M9, M10	ABC IT administrator

[a] See Measures table.

Verification

Unless otherwise specified, the following verification activities are performed externally to (or independently of) the process:[7]

- Audits are conducted periodically to verify that data in physical form has been securely transported and stored in accordance with requirements.
- Audits are conducted periodically to verify that data in digital form has been securely stored and shared in accordance with requirements.
- Scripts are run against SharePoint sites periodically to verify that attempts to access data by unauthorized parties fail.
- If data is restored, it is successfully restored in the requested version to the correct access-controlled SharePoint site.
- The ability to restore data from backups is regularly tested.
- The ABC team lead verifies that data is returned or destroyed in accordance with requirements.

[7] Verification roles are not identified due to verification activities being performed externally to the process. If such activities are performed internally to the process, roles should be identified here.

Measures

The following candidate[8] measures apply to the handling of most data types. Variations or new measures that apply to a specific type of data are defined in the applicable procedure for that data type.

ID	Measure	Type of Information	Measure Type	Base or Derived	Activities	Applicable SG.SP
DH-M1	Elapsed time between creation or receipt of data and delivery of data final report (mean, median)	Final report	Implementation	Base of type schedule	1.0, 5.0	GG2.GP2 GG2.GP8
DH-M2	Number of violations of access control requirements or policies for data • As a result, number of successful intrusions into technology assets (digital data) or facility assets (physical data) where data are stored, processed, and transmitted • As a result, number of instances of data being accessed in an unauthorized manner • As a result, number of incidents declared • As a result, number of breaches of confidentiality and privacy of data • As a result, number of violations of requirements for data	Data intrusions Data violations	Implementation; possibly Effectiveness	Base of type count	Physical data: 2.0, 3.0, 6.0 Digital data: 3.0–6.0	KIM:SG4.SP2 KIM:SG5.SP1 GG2.GP8
DH-M3	Number of violations of data handling requirements	Requirements	Implementation	Base of type count	1.0–6.0	KIM:SG4, SG5, SG6
DH-M4	Difference in planned versus actual schedule (number of days) to perform the data handling process[a]	Plan Procedure activities	Implementation; possibly Effectiveness	Derived	Planned: project work plan[b] Actual: 1.0, 6.0	GG2.GP2 GG2.GP8

[a] The base measures from which this derived measure is calculated are the number of days between the planned process start date and the planned process end date compared with the number of days between the actual process start date and the actual process end date (see also DH-M8).

[b] The project work plan is developed outside of this process definition. It describes the activities, schedule, and costs for the engagement that results in the data handled by this process and its supporting procedures.

[8] Measurement can be time consuming and expensive. Organizations should select those measures that are most meaningful to inform decisions and affect behaviors related to improving process performance and meeting management objectives.

Measures (continued)[9]

ID	Measure	Type of Information	Measure Type	Base or Derived	Activities	Applicable SG.SP
DH-M5	Difference in planned versus actual cost to perform the data handling process[c]	Plan Resources	Implementation; possibly Effectiveness	Derived	Planned: project work plan Actual: monthly financial reports	GG2.GP2 GG2.GP8
DH-M6	Number of instances of data received or created	Data receipt	Implementation	Base of type count	1.0	ADM:SG1.SP1 ADM:SG3.SP2 GG2.GP8
DH-M7	Number of instances of data returned or destroyed	Data return or destruction	Implementation	Base of type count	6.0	ADM:SG1.SP1 ADM:SG3.SP2 GG2.GP8
DH-M8	Elapsed time between creation or receipt of data and the return of the data to its owner and/or its destruction in any ABC facility or on any ABC technology asset (mean, median)	Data return or destruction	Implementation	Base of type schedule	1.0, 6.0	ADM:SG1.SP1 ADM:SG3.SP2 GG2.GP8
DH-M9	Elapsed time (from initial request) to recover data from backups (mean, median)	Data sustainment	Implementation	Base of type schedule	8.0	KIM:SG6.SP1 GG2.GP8
DH-M10	Percentage of data recovered that does not match the most current version of data backed up (should be 0%)	Data sustainment	Implementation	Derived	8.0	KIM:SG6.SP1 GG2.GP8

[c] The base measures from which this derived measure is calculated are the estimated cost of effort, travel, and other related expenses compared with the actual cost as of the process end date.

[9] The definition of each table column and column entry and further details of how each measure is collected, analyzed, and reported (including to whom and key stakeholders) are documented in Allen [2010].

Exit Criteria

- Data has been protected and sustained in accordance with requirements.
- Data has been returned or destroyed in accordance with requirements.

Referenced Sources

[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

TEMPLATE

[Name] Process Definition

Purpose

The purpose of the [process name] process is…

Scope

This process applies to...

Acronyms and Definitions

ACR1	Definition
ACR2	Definition

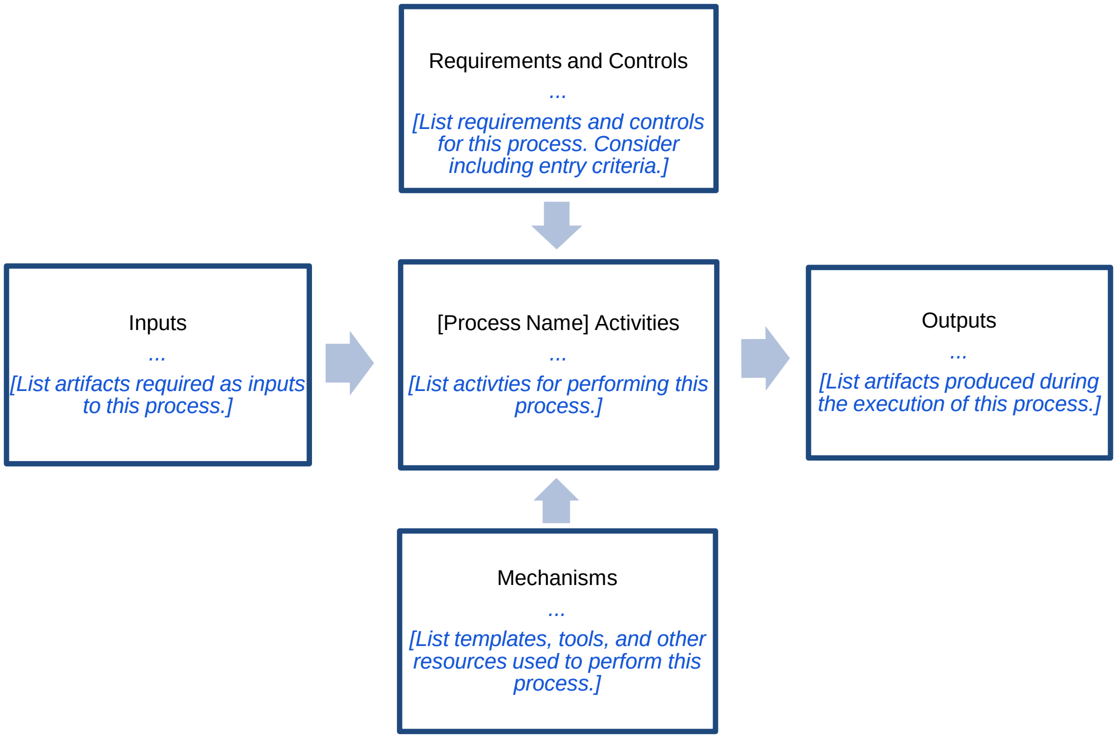
Outputs

[List the expected work product(s) produced from the activities of the process.]

•

Context Diagram

[If desired, show the context within which process activities occur.]


Requirements and Controls
...
[List requirements and controls for this process. Consider including entry criteria.]
Inputs
...
[List artifacts required as inputs to this process.]
[Process Name] Activities
...
[List activties for performing this process.]
Outputs
...
[List artifacts produced during the execution of this process.]
Mechanisms
...
[List templates, tools, and other resources used to perform this process.]

Entry Criteria

[List the conditions that must be met for the process to begin.]

-

Inputs

[List the expected inputs to the process.]

-

Requirements

[List the requirements relevant to the process, including externally imposed requirements such as standards, laws, and regulations, or reference a separate source, such as an asset profile.]

Controls

[List the controls that are used to satisfy the requirements for the process in the following categories.]

-

Policies
[List the relevant policies for the process.]

Procedures
[List the procedures referenced in this process or that derive from the process.]

Standards
[List the relevant standards for the process.]

Methods and Technologies
[List the relevant methods and technologies for the process.]

Training
[List the training required for the process.]

Mechanisms

[List the mechanisms used to aid in the implementation of the process.]

Guidelines
[List the relevant guidelines for the process.]

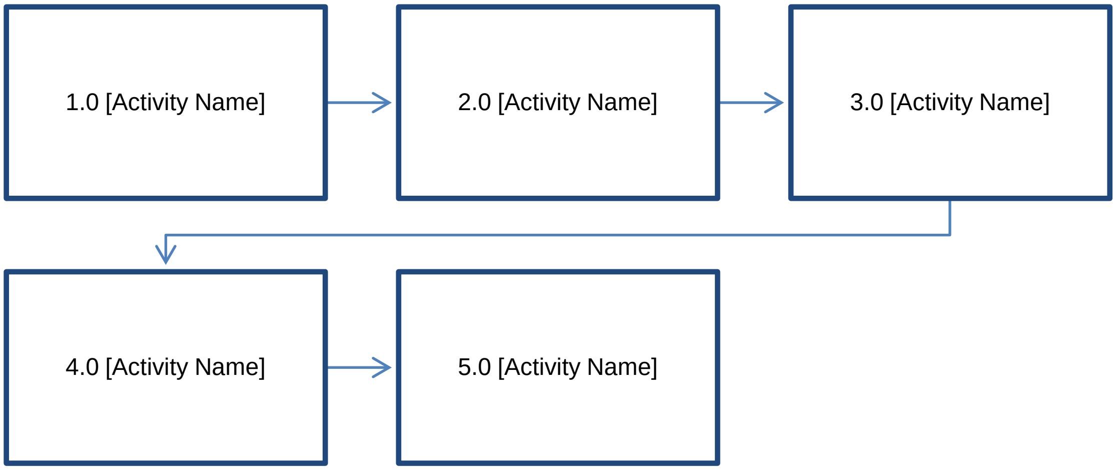
Templates
[List the templates used in the process.]

Checklists
[List the checklists referenced in the process.]

Tools
[List the tools used to implement the process.]

Process Flow Diagram

[If desired, show the sequence of activities that compose the process.]



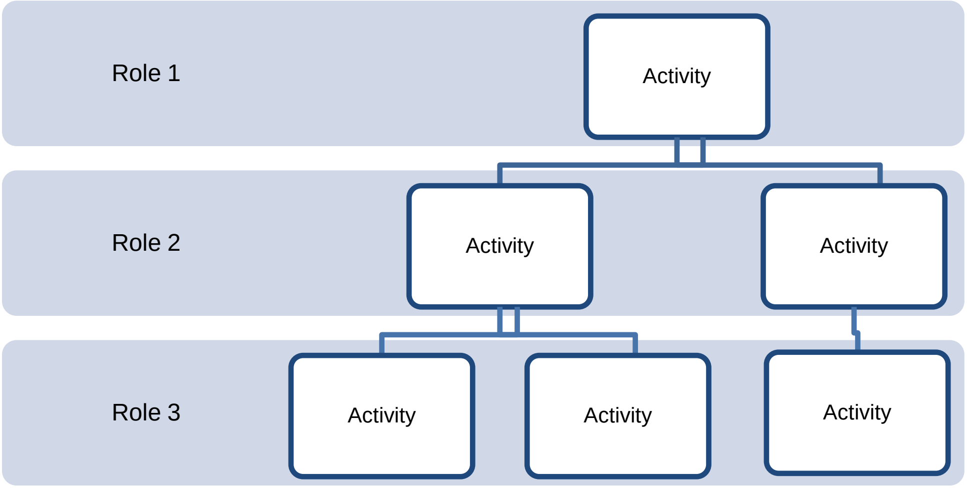
Roles

[Describe the roles that perform the process.]

Role	Description	Responsibility
[role name]	[role description]	[responsibilities of the role]

Swim Lane Diagram

[If desired, show the relationship of roles responsible for performing process activities.]



Activities

[Describe the activities that compose the process.]

Activity No.	[Process Name] Activities	Description	Applicable Measures[a]	Role
[sequential number]	[activity name]	[activity description]	[measure ID]	[role performing the activity]

[a] See Measures table.

Verification

[Describe the verification activities that are necessary to confirm that the activities of the process have been adequately performed.]

The following verification activities are performed external to (or independent of) the process:

-

Measures[10]

[Describe the measures used to support management information needs for the process.]

ID	Measure	Type of Information	Measure Type	Base or Derived	Activities	Applicable SG.SP

[ID: A unique, sequential identifier assigned to each measure.]

[Measure: Measure description.]

[Type of Information: A category that can be used for affinity grouping of related measures. These can be work products (such as asset inventory and asset controls) or activities (such as change management and obligation satisfaction).]

[Measure Type: Implementation, effectiveness, or process performance.]

[Base or Derived: A base measure is a directly observable attribute of an asset, service, or resilience process; a derived measure is a mathematical function of two or more base and/or derived measures.]

[Activities: Assigned numbers of the activities in which the measure is collected.]

[Applicable SG.SP: Related specific goal and specific practice in CERT-RMM.]

[For further definition of each column in the measures table, see Chapter 3 in Allen [2011].]

Exit Criteria

[List the conditions that must be satisfied for the process to be considered complete.]

-

Referenced Sources

[List additional sources that are referenced in the process.]

[10] Further details of how each measure is collected, analyzed, and reported are documented in Allen [2010].

Appendix B: Procedure Definition Example and Template

EXAMPLE

This fictitious example is a procedure for handling survey data submitted to ABC Organization by an external party. It is subordinate to the Data Handling process shown in Appendix A.

Survey Data Handling Procedure Definition

Procedure Purpose

The purpose of the Survey Data Handling procedure is to protect and sustain designated survey data in accordance with external party requirements and ABC Organization polices and standard practices.

Scope

This procedure applies to all designated survey data handled by the ABC Organization Survey Team.

Acronyms and Definitions

CERT-RMM	CERT Resilience Management Model
EP	External party staff member
AST	ABC Organization Survey Team

Outputs

Resilient (protected and sustained) survey data

Entry Criteria

Survey data is created or received.[11]

Inputs

Survey data from external parties

References

Processes
Data Handling Process

Requirements
Refer to Survey Data Information Asset Profile [see Appendix C].

[11] Data creation begins the moment survey data is recorded or shared in physical form or digital form.

Roles

The following roles apply to the handling of all survey data:

Role	No. of People	Description	Responsibility
AST	1–4	ABC staff member who participates in one or more surveys. Includes the survey team lead and co-lead.	Acts as custodian of survey data
AST lead and co-lead	1–2	Leader and co-leader of the team that conducts a specific survey	Manage survey program (schedules, budget, tasking, etc.); manage the conduct, data collection, reporting, and measurement associated with a specific survey
EP	1–4	Staff member from an external party organization	Owner of survey data; participates in surveys; develops, presents, and provides survey data
ABC editor	1	Technical editor	Edits the final survey report
ABC IT administrator	Several	IT staff member who backs up and restores survey data residing on SharePoint servers	Performs regular backups and tests ability to restore from backups; ensures that survey data that resides on SharePoint servers is encrypted

Activities

The activities for handling survey data are described in the table below. Activities are as described in the Data Handling Process Definition. Unless otherwise indicated, AST members execute all activities.

Activity	Description
1.0 Create or receive the data	Survey data is obtained during survey meetings, via survey-related email, and via postings to access-controlled SharePoint sites.
2.0 Transport the data	Survey data that is provided in physical form during a survey meeting is securely transported from the survey location to an AST member’s office.
3.0 Store the data	Survey data in digital form is stored on access-controlled SharePoint sites. Survey data in physical form is stored in a locked desk or file cabinet after the completion of the survey meeting where the data was provided.
4.0 Share and access the data (internal to the ABC Organization)	Survey digital data is accessed from access-controlled SharePoint sites. Survey data (in digital and physical form) can be accessed only by designated EP staff (external SharePoint site) and AST members (external and internal SharePoint site).
5.0 Deliver the data (to the EP)	Final encrypted data (such as reports and presentations), prepared by an ABC editor, are sent to the EP via email.
6.0 Destroy or return the data	Survey data in physical form is returned within 30 days of the end of the survey project. Survey data in digital form is destroyed within 30 days of the end of the survey project. Destruction is confirmed with the EP.
7.0 Back up the data	ABC IT administrators regularly back up SharePoint servers where survey data in digital form resides.
8.0 Restore the data from backups	Upon AST lead or co-lead request, data is restored to access-controlled SharePoint sites as needed. ABC IT administrators regularly test the ability to restore data from backups.

Verification

The verification activities for this procedure include the following:

- Audits are conducted periodically to verify that survey data in physical form has been securely transported and stored in accordance with requirements.
- Audits are conducted periodically to verify that survey data in digital form has been securely stored and shared in accordance with requirements.
- Scripts are run against SharePoint sites periodically to verify that attempts to access survey data by unauthorized parties fail.
- If survey data is restored, it is successfully restored in the requested version to the correct access-controlled SharePoint site.
- The ability to restore survey data from backups is periodically tested in accordance with ABC Organization service level agreements.
- The ABC team lead verifies that survey data is returned or destroyed in accordance with EP requirements.

Measures

The following measures from the Data Handling Process apply to this procedure. The ID field shows the process measure ID and assigns a new procedure measure ID, for traceability.

ID	Measure	Type of Information	Measure Type	Base or Derived	Activities	Applicable SG.SP
DH-M2 SDH-M1	Number of violations of access control requirements or policies for survey data • As a result, number of successful intrusions into technology assets (digital data) or facility assets (physical data) where survey data is stored, processed, and transmitted • As a result, number of instances of survey data accessed in an unauthorized manner • As a result, number of incidents declared • As a result, number of breaches of confidentiality of survey data • As a result, number of violations of requirements for survey data	Data intrusions Data violations	Implementation; possibly Effectiveness	Base of type count	3.0, 4.0, 6.0	KIM:SG4.SP2 KIM:SG5.SP1 GG2.GP8
DH-M3 SDH-M2	Number of violations of survey data handling requirements	Requirements	Implementation	Base of type count	1.0, 3.0, 4.0, 6.0	KIM:SG4, SG5, SG6
DH-M6 SDH-M3	Number of instances of survey data received or created	Data receipt	Implementation	Base of type count	1.0	ADM:SG1.SP1 ADM:SG3.SP2 GG2.GP8
DH-M7 SDH-M4	Number of instances of survey data returned or destroyed	Data return or destruction	Implementation	Base of type count	6.0	ADM:SG1.SP1 ADM:SG3.SP2 GG2.GP8
DH-M8 SDH-M5	Elapsed time between creation or receipt of survey data and the return of the data to the survey owner and/or its destruction in any ABC facility or on any ABC technology asset (mean, median)	Data return or destruction	Implementation	Base of type schedule	1.0, 6.0	ADM:SG1.SP1 ADM:SG3.SP2 GG2.GP8
DH-M9 SDH-M6	Elapsed time (from initial request) to recover survey data from backups (mean, median)	Data sustainment	Implementation	Base of type schedule	8.0	KIM:SG6.SP1 GG2.GP8
DH-M10 SDH-M7	Percentage of survey data recovered that does not match the most current version of survey data backed up (should be 0%)	Data sustainment	Implementation	Derived	8.0	KIM:SG6.SP1 GG2.GP8

Exit Criteria

- Survey data has been protected and sustained in accordance with requirements.
- Survey data has been returned or destroyed in accordance with requirements.

TEMPLATE

[Name] Procedure Definition

Purpose

The purpose of the [procedure name] procedure is…

Scope

This procedure applies to...

Acronyms and Definitions

ACR1	Definition
ACR2	Definition

Outputs

[List the expected work product(s) produced from the activities of the procedure.]

•

Entry Criteria

[List the conditions that must be met for the procedure to begin.]

•

Inputs

[List the expected inputs to the procedure.]

•

References

[List any documents and sources that guide the performance of the procedure. The procedure inherits all Requirements and Controls from its parent process unless otherwise stated.]

Policies

[List the relevant policies, acts, or regulations for the procedure.]

Processes

[List the processes that the procedure supports.]

Requirements

[List or reference the requirements relevant to the procedure.]

Standards

[List the relevant standards for the procedure.]

Guidelines

[List the relevant guidelines for the procedure.]

Templates
[List the templates used in the procedure.]

Checklists
[List the checklists used in the procedure.]

Training
[List the training required for the procedure.]

Tools
[List tools used to implement the procedure.]

Roles

[Describe the roles that perform the procedure.]

Role	Number of People	Description	Responsibility
[role name]	[number range]	[role description]	[responsibilities of the role]

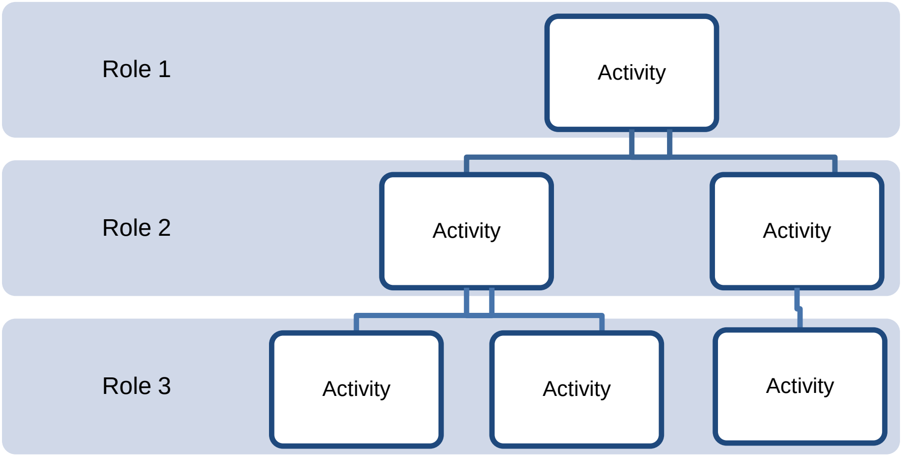
Activities

[Describe the activities that compose the procedure.]

Activity	Description
[activity number and name—each activity should map directly to one or more activities in the parent process definition]	[activity description, including the role(s) performing each sub-activity]

Swim Lane Diagram

[If desired, show the relationship of roles responsible for performing procedure activities.]



Verification

[Describe the verification activities that are necessary to confirm that the activities of the procedure have been adequately performed.]

The verification activities for the [procedure name] include the following:

-

Measures

[Describe the measures used to support management information needs for the procedure.]

ID	Measure	Type of Information	Measure Type	Base or Derived	Activities

[ID: A unique, sequential identifier assigned to each measure.]

[Measure: Measure description.]

[Type of Information: A category that can be used for affinity grouping of related measures. These can be work products (such as asset inventory and asset controls) or activities (such as change management and obligation satisfaction).]

[Measure Type: Implementation, effectiveness, or process performance.]

[Base or Derived: A base measure is a directly observable attribute of an asset, service, or resilience process; a derived measure is a mathematical function of two or more base and/or derived measures.]

[Activities: Assigned numbers of the activities in which the measure is collected.]

[For further definition of each column in the measures table, see Chapter 3 in Allen [2011].]

Exit Criteria

[List the conditions that must be satisfied for the procedure to be considered complete.]

-

Appendix C: Information Asset Profile Example and Template

The information asset profile template in this section is a compilation of unpublished profile templates created by members of the Resilient Enterprise Management team and from profile information in the following sources:

- *CERT® Resilience Management Model* [Caralli 2011]
- *Introducing OCTAVE Allegro* [Caralli 2007]
- *Information Asset Profiling* [Stevens 2005]

The profile illustrates how an asset definition can

- link an information asset to the services in which it is used, to help ensure that any service-specific requirements are considered in the development of resilience requirements for the asset
- list all of the ways in which the asset is stored, transported, and processed, to help ensure that all forms and locations of the asset are considered in the development of resilience requirements
- specify the asset's resilience requirements

The example and template do not include a field for the value of the asset in either qualitative or quantitative terms. See Stevens [2005], pages 39–41, for guidance on developing an information asset valuation.

The profile could be adapted for other asset types, such as technology assets and facilities. The profile can also be customized for specific uses. The example contains three fields that are not in the template but that are needed to fully describe the asset: data collection objective, how collected and by whom, and collection frequency.

Survey Data Information Asset Profile

Profile date and version	September 17, 2011; v 0.1
Profile creator	Jerry Brekovny
Data set name	Survey Data
Data set description	Data that external party (EP) staff provide to ABC Organization during their participation in a survey project. Data may include presentations, reports, templates, process definitions, survey responses and observations, and other artifacts that EP staff provide.
Data collection objective	The objective is to understand how the EP intends to use and is using CERT-RMM to improve its organization's operational resilience to meet a specific improvement project objective.
How collected and by whom	Developed and provided by EP staff members to members of the ABC Organization Survey Team (AST). The AST lead or co-lead takes possession of all survey data provided at each survey meeting and between survey meetings via email and SharePoint.
Collection frequency	Survey data is collected at each survey meeting and between survey meetings via email or posts to designated SharePoint sites.
Primary use	Provides essential information to guide the EP in meeting their improvement project objective.
Other acceptable uses	Improvement of ABC's CERT-RMM-based processes and process assets; improvement of ABC's survey process
Data owner	EP organizations
Services that use this asset	Not applicable

Where stored (including backups and duplicates)	*Form*	*Device and location*	*Custodian*
	Email	MS Outlook email server	ABC IT administrator
	Email	Local mail on AST laptops	AST lead or co-lead AST member
	Email	Local mail on AST desktop machines	AST lead or co-lead AST member
	Survey data (physical)	Locked file cabinet or desk in a AST member's office	AST lead or co-lead AST member
	Survey data (digital)	SharePoint server (internal) SharePoint server (external)	AST lead or co-lead AST member ABC IT administrator
	Survey data (digital)	AST laptops	AST lead or co-lead AST member
	Survey data (digital)	AST desktops	AST lead or co-lead AST member

Where processed	*System or application*	*Custodian*	
	MS Office 2007 (Word, PowerPoint, Excel)	AST lead or co-lead AST member	
	MS Outlook 2007	AST lead or co-lead AST member	
How transported	*Form*	*Device or method*	*Custodian*
	Email messages	Email; MS Outlook 2007	AST lead or co-lead AST member
	Survey data (paper)	By hand, from EP meeting site to office	AST lead or co-lead AST member
	Survey data (digital)	Email attachment; MS Outlook 2007	AST lead or co-lead AST member
	Survey data (digital)	Laptop, between office and home	AST lead or co-lead AST member
	Survey data (digital)	SharePoint server (external)	AST lead or co-lead AST member
Sensitivity category	Unclassified sensitive		

Resilience requirements and strategies	*Confidentiality requirements*	*Confidentiality strategy*
	ABC Organization Code of Business Ethics and Compliance requirements for controlled information	AST members (including AST lead and AST co-lead) and all ABC staff members who participate in survey projects understand by agreement that no survey data is to be shared with anyone other than survey participants without explicit, written member permission. Only AST members have access to survey data.
	Integrity requirements	*Integrity strategy*
	ABC Organization Code of Business Ethics and Compliance requirements for controlled information	Same access controls used for confidentiality strategy.
	Availability requirements	*Availability strategy*
	Survey data must be accessible on SharePoint from 6:00 a.m. to 11:00 p.m. daily. Survey data must be retrievable via restore from backup.	The SharePoint site is available 24/7. Digital data is backed up by ABC IT in accordance with the posted service level agreement. All backups are encrypted. The ability to restore digital data from backups is regularly tested in accordance with the posted service level agreement.
	Privacy requirements	*Privacy strategy*
	None	Not applicable
	Other requirements	*Strategy*
	As identified by EP staff for specific survey data	Same as confidentiality strategy.

Information Asset Profile Template

Profile date and version	Create a version number that follows a standard, enterprise-wide convention.
Profile creator	Name, role or position, and contact information of the person or persons who wrote the profile.
Data set name	Descriptive name for the data set (not a file name).
Data set description	Describe the contents of the information asset in enough detail to ensure that the boundaries of the asset are clear. (See Stevens [2005], pages 25–28, for further information.)
Primary use	Describe the primary purpose for which the asset is used.
Other acceptable uses	Describe secondary purposes for which the asset is used (if applicable, the *only* other purposes for which it may be used).
Data set owner	Role or position and department; organization name if it is an external entity; and contact information for the person currently acting in the role.
Services that use this asset	*Services* is used in the sense of “activities that the organization carries out in the performance of a duty or in the production of a product” [Caralli 2011]. An IT service, for example, might be help desk support; an information asset used in that service might be the service request database.

Where stored (including backups and duplicates)	*Form*	*Device and Location*	*Custodian*
	A single information asset may be instantiated in many forms (Access database, Excel file, PDF, HTML file, paper copy, etc.). Include a Form/Device and Location/Custodian row for each form of the asset.	Device type (server, laptop, PDA, tape, CD, USB flash drive, safe, etc.) and any name or other identifier, and, as applicable, device location—physical (such as a room number and a building name and address) and/or virtual (such as a SharePoint library address).	"Asset custodians are persons or organizational units, internal or external to the organization, that agree to and are responsible for implementing and managing controls to satisfy the resilience requirements of high-value assets while they are in their care" [Caralli 2011, pg. 33]. Enter the custodian's role/position and department; organization name if it is an external entity; and contact information for the person currently acting in the role.
Where processed	*System or application*	*Custodian*	
	Systems and applications are temporary "containers" of data and should therefore be considered in the development of resilience requirements for the asset.	Same as above.	
How transported	*Form*	*Device or method*	*Custodian*
	Same as above.	Network or network segment (specify wired or wireless), email application, FedEx, etc.	Same as above.
Sensitivity category	"*Sensitivity* is a measure of the degree to which an information asset must be protected based on the consequences of its unauthorized access, modification, or disclosure" [Caralli 2011, pg. 514]. Specify the appropriate category from your organization's information asset sensitivity categorization scheme, if applicable. Examples of sensitivity categories are public, internal use only, confidential, proprietary, and secret.		

Resilience requirements and strategies	*Confidentiality requirements*	*Confidentiality strategy*
	Specify all requirements related to restricting access to the asset to authorized people, processes, and devices, citing any relevant policies, rules, laws, and regulations to which the asset is subject.	List the administrative, technical, and/or physical controls that are required to meet the specified confidentiality requirements.
	Integrity requirements	*Integrity strategy*
	Specify all requirements related to maintaining the asset in the condition intended by its owner so it will continue to be useful for the purposes intended by the owner, citing any relevant policies, rules, laws, and regulations to which the asset is subject.	List the administrative, technical, and/or physical controls that are required to meet the specified integrity requirements.
	Availability requirements	*Availability strategy*
	Specify all requirements related to ensuring that the asset is accessible to authorized users (people, processes, and devices) whenever it is needed, citing any relevant policies, rules, laws, and regulations to which the asset is subject.	List the administrative, technical, and/or physical controls that are required to meet the specified availability requirements.
	Privacy requirements	*Privacy strategy*
	Specify all requirements related to ensuring that information about individuals is disclosed only to people, processes, and devices authorized by those individuals or permitted under privacy laws and regulations.	List the administrative, technical, and/or physical controls that are required to meet the specified privacy requirements.
	Other requirements	*Strategy*
	Enter any requirements that don’t fit in the previous categories, such as unique requirements arising from contractual specifications for resilience.	List the administrative, technical, and/or physical controls that are required to meet other requirements.

Appendix D: Alternative Process or Procedure Example and Template

One of the members of the CERT-RMM Users Group generously shared a generic template derived from what they use for both process and procedure definitions, along with an Asset Definition Process example. The example appears first, followed by the template.

Process

Asset Definition

Copyright 2011	**A hard copy of this document may not be current. The current issue is on the Company Intranet.**
Issue:	1
Effective:	April 2011
Approval:	Director, Engineering Assets
Controlled by:	Engineering Review Board
Process Owner:	Asset Management Group (Point of Contact email address)

PURPOSE

The purpose of this process is to ensure that Engineering groups identify and document organizational assets to ensure sustained productivity to support Engineering services.

SCOPE & APPLICABILITY

This process applies to every group within the Engineering organization.

GENERAL

Identifying and documenting high value organizational assets is critical to ensuring a sustainable organization, especially in times of adversity and risk.

RESPONSIBILITIES

Engineering Manager

1. Identify and document group’s involvement in critical services
2. Identify and document assets, including people, information, technology and facilities
3. Review assets with team
4. Get approval from Engineering Review Board for new and updated assets

Engineering Group

1. Review assets documented by Engineering Manager

Engineering Review Board

1. Review and approve assets documented by Engineering Manager
2. Identify and document conflicts and dependencies between Engineering Groups.

ENTRY CRITERIA

1. Senior Executive Management has identified or updated high-value Engineering services as defined in the yearly goals and objectives.

INPUT

1. Organizational charts
2. Support Systems Database

IMPLEMENTATION

On a yearly basis, or when Senior Executive Management updates the goals and objectives:

1. The **Engineering Manager** identifies the Engineering Group's involvement in critical services and documents this involvement in a Mission Statement.
2. For each critical service, the **Engineering Manager** identifies the critical staff for performing that service, including name, employee number, role in providing the service, and position in the organization (or in another organization). Critical staff is documented in the Support Systems Database.
3. For each critical service, the **Engineering Manager** identifies any information required by the service. This includes any records, files, processes and procedures needed to provide the service. The protection level of this information must also be identified (i.e., no restrictions, sensitive, proprietary, confidential, export controlled, or a combination) as well as the location (URL, SharePoint address, or physical location) and the organizational owner of the information. Critical information is documented in the Support Systems Database, including a brief description of the information.
4. For each critical service, the **Engineering Manager** identifies any tools or applications needed in performing the critical service. This would include any databases, automated forms, software, hardware, or COTS used. It does not need to go to the server or cable level (these assets are identified by the Computer Services organization). The location of the tool or application (URL, SharePoint address, or physical location) must be identified, as well as the organizational owner of the tool / application. Critical technology assets are documented in the Support Systems Database.
5. If there are facilities used for the critical services that are *not provided by the company* (i.e., work in non-company owned facilities), the **Engineering Manager** identifies these facilities in the Support Systems Database. (Company owned facilities are identified by the Facilities organization.) This will include the address, facility owner, location within the facility, and requirements for entry into the facility.
6. Once documented in the Support Systems Database, the **Engineering Manager** will review the entries with her/his **Engineering Group** to ensure both correctness and communication. The Engineering Manager will then submit new items or updates to the Engineering Review Board for review and approval.
7. The **Engineering Review Board** will review the new or updated items in the Support Systems Database. This review will be done for correctness, consistency of approach and the identification of any conflicts or dependencies with other Engineering groups.

OUTPUT

1. Mission Statement
2. Updates to Support Systems Database

EXIT CRITERIA

1. Engineering Review Board approves the new and updated entries in the Support Systems Database.

MEASUREMENTS

1. Number of staff assets changed (modified, added and deleted)
2. Number of information assets changed (modified, added and deleted)
3. Number of technology assets changed (modified, added and deleted)

4. Number of facilities assets changed (modified, added and deleted)

INFORMATION LINKS

Process Assets:

- ENG120, Engineering Review Board Submittal Process

Sources and References:

- Corporate Policy, 123 Resource Identification and Protection

General Information:

- CERT® Resilience Management Model, Version 1.1

REVISION HIGHLIGHTS

Issue	Published	Author	Summary of Improvements
1	**April 2011**	**I.M. Theauthor**	**New document**

Process or Procedure Template *Replace with "Process" or "Procedure" or similar heading (i.e., there may be cases where this is a form or checklist rather than a process or procedure)*

TITLE

Replace "Title" with a descriptive title for this process element (note that process element will be used as a generic term to refer to either the Process or the Procedure). Also put this Title in "Subject" box of File/Properties.

Copyright 2011 *{optional}*	**A hard copy of this document may not be current. The current issue is on the *{add location}*.**

Issue:	*<If this is a new process element, leave the Issue number as "1". If this is a revision, increment the number by 1.>*
Effective:	Date *< Use the following format for the effective date: Month, Year e.g., February 2009>*
Approval:	*{Position that approves the process / procedure}*
Controlled by:	*{Position that controls the process / procedure}*
Process Owner:	*{Position that owns the process / procedure}* (Point of Contact email address)*Insert the email address of the Point of Contact to whom you want suggestions and revision update notices sent. Also put this name in "Author" box of File/Properties.>*

PURPOSE

Describe why this process or procedure is needed in two sentences or less. Include a reference to any policy that this process or procedure implements.

SCOPE & APPLICABILITY

Describe the scope of the process or procedure (e.g., applies to all employees, applies to a particular role or activity within a function, etc.)

GENERAL

This section includes any information which is helpful in understanding the context for the process element but is not explicitly a part of the process element. Background information, clarifications, and specific terms used in the asset may be included. Note that definitions can be added here.

- *A Process is "what" to do – a Set of interrelated or interacting activities which transforms inputs into outputs.*
- *A Procedure is "how" to do it – a logical set of instructions to carry out an activity or process.*

RESPONSIBILITIES

This section lists the responsibilities of the agents that have a role in the activities or instructions listed in the Implementation section.

Responsible Party #1*Replace " Responsible Party #1" with the role of **WHO** is primarily responsible for some or all of the implementation of this process element*.

1. Responsibilities *Replace " Responsibilities" with actual responsibilities for this WHO.*

Other Responsible Party *Replace " Other Responsible Party" with a role of another WHO (if applicable) that is responsible for parts of this process element. This is usually the **WHO** that has some supporting role in this process element. List as many as necessary.*

1. Responsibilities. *Replace " Responsibilities" with actual responsibilities for this other **WHO**.*

ENTRY CRITERIA

1. *This section states conditions that should exist before process element execution.*

INPUT

1. *This section lists the artifacts and sources that may be required or be of assistance in performing the activities.*

IMPLEMENTATION

1. *This section describes activities and directions with details of how to, when, where and by whom. A process flow diagram can be added for clarification of the implementation.*

OUTPUT

1. *This section lists the artifacts produced by the activities and their destination.*

EXIT CRITERIA

1. *This section states conditions that should exist for the process element to terminate.*

MEASUREMENTS

1. *This section contains measures that should be obtained during process element execution to measure policy or process effectiveness. This section should state the measurement definition and when it should be obtained. The measurement data should be collected, tracked and made available for process improvement.*

INFORMATION LINKS

Process Assets:

- Titles *Insert TITLES of process elements (policy, process, procedure, instruction or form) that help implement, support or relate to this process or procedure. Provide a link to the asset as well as the title. Note: If any process element is not available via a link, provide the name and phone number of a point of contact from whom a copy can be obtained.*

Sources and References:

- Titles *Insert TITLES of a source which caused the issuing of this process element (e.g., Corporate policy) or a reference that is embedded in the text of this process element. Provide a link to the asset as well as the title. Note: If any of these are not available via a link, provide the name and phone number of a point of contact from whom a copy can be obtained.*

General Information:

- Titles and Links - *Insert the TITLES and LINKS of any documents or data that provide general information on the subject matter of the process element. This might be a link to the home page of the process owner of this process element or another related organizational home page, e.g., Software Engineering Institute, IEEE or a government regulatory site.*

REVISION HIGHLIGHTS

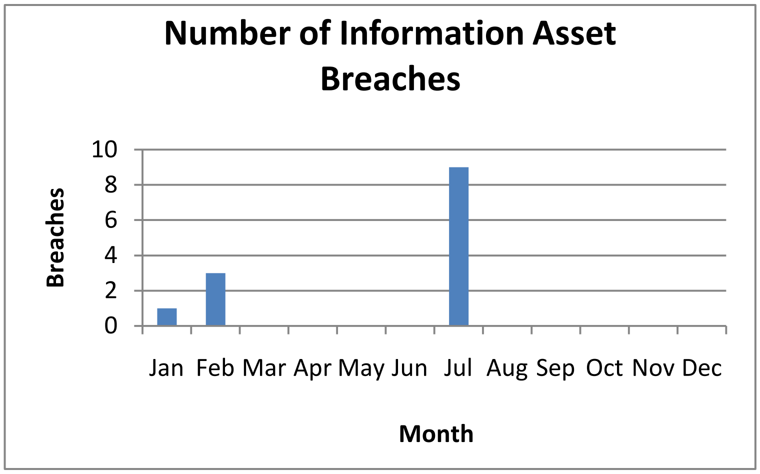
Issue	Published	Author	Summary of Improvements
#	**Same as the effective date at the top of the template**	**Name**	**New document or, if a revision, provide a summary of the changes**

APPENDICES*

It is recommended to use the Information Links section or create a form instead of using an appendix. However, appendices could contain additional information to implement this process element e.g., checklists, computer tools and utilities, etc.

Appendix E: Measure Definition Example and Template

Example for Derived Measure[12] DH-M2 from the Data Handling Process

Measure Name and ID	Number of breaches of confidentiality and privacy traced to violations of access control policies for information assets (DH-M2)	
Goal	Protect designated data	
Question(s)	How many breaches of confidentiality and, if applicable, privacy occurred as a result of unauthorized access of designated data in a specific time period?	
Related Processes and Procedures	Data Handling Process Survey Data Handling Procedure Diagnostic Data Handling Procedure Performance Data Handling Procedure	
Visual Display		
Data Input(s) **Data elements** **Data type**	Start date of last reporting period	Base measure of type “schedule”
	End date of last reporting period	Base measure of type “schedule”
	Root causes of incidents	
Data Collection **How** **When/how often** **By whom**	• On an event-driven basis, the organization’s service desk personnel and CSIRT collect information about an incident throughout its life cycle. • Information is reviewed either when the incident is closed (*IMC:SG4.SP4 Close Incidents*) or when the post-incident review is performed (*IMC:SG5.SP1 Perform Post-Incident Review*). • The CSIRT maintains a list of root causes of incidents and updates it after each post-incident review. • Information about information assets is maintained in the asset	

[12] Allen [2010] provides a template for defining base measures.

<table>
<tr><td></td><td>inventory/database/profiles (<em>ADM:SG1 Establish Organizational Assets; KIM:SG1 Establish and Prioritize Information Assets; TM:SG1 Establish and Prioritize Technology Assets</em>).</td></tr>
<tr><td><strong>Data Reporting</strong>
<strong>By/to whom</strong>
<strong>When/how often</strong></td><td>• The CSIRT reports data to the CISO.
• Data is reported once per reporting period.</td></tr>
<tr><td><strong>Data Storage</strong>
<strong>Where</strong>
<strong>How</strong>
<strong>Access control</strong></td><td>• Data is stored in the incident knowledgebase and asset database.
• Each incident report record contains root cause information.
• Each incident report record contains information about the asset affected.
• Everyone has read access to the incident knowledgebase and asset database.
• Only CSIRT has write access to the incident knowledgebase.
• Only asset custodians and asset owners have write access to the asset database.</td></tr>
<tr><td><strong>Stakeholders</strong>
<strong>Information owner(s)</strong>
<strong>Information customer(s)</strong></td><td>• The CISO is the owner of the incident knowledgebase.
• The CISO and senior management are the customers for this information.
• The incident owner is responsible for maintaining and presenting all information related to an incident.
• Asset custodians are responsible for maintaining and presenting all information related to an information asset and the technology asset(s) on which the incident occurs.
• The staff assigned to incident management are responsible for executing the incident management process <em>(IMC:SG1.SP2 Assign Staff to the Incident Management Plan)</em>.</td></tr>
<tr><td><strong>Algorithm or Formula</strong></td><td>Each incident record in the incident knowledgebase must contain the following information:
<table>
<tr><th>Variable</th><th>Type</th></tr>
<tr><td>Date of occurrence</td><td>Date</td></tr>
<tr><td>Assets, services, and organizational units affected by incident</td><td>Asset ID, service ID, organizational unit ID</td></tr>
<tr><td>Root cause</td><td>Name or label</td></tr>
</table>
Other information needed:
<table>
<tr><th>Variable</th><th>Type</th></tr>
<tr><td>Start of reporting period</td><td>Date</td></tr>
<tr><td>End of reporting period</td><td>Date</td></tr>
<tr><td>Reporting interval</td><td>Quarter, month, or week</td></tr>
<tr><td>List of root causes</td><td>Names or labels</td></tr>
<tr><td>List of assets</td><td>Names or IDs</td></tr>
<tr><td>Number of breaches</td><td>Zero or positive integer</td></tr>
</table></td></tr>
</table>

Algorithm steps to create input values

For each root cause in the organization’s list of root causes:

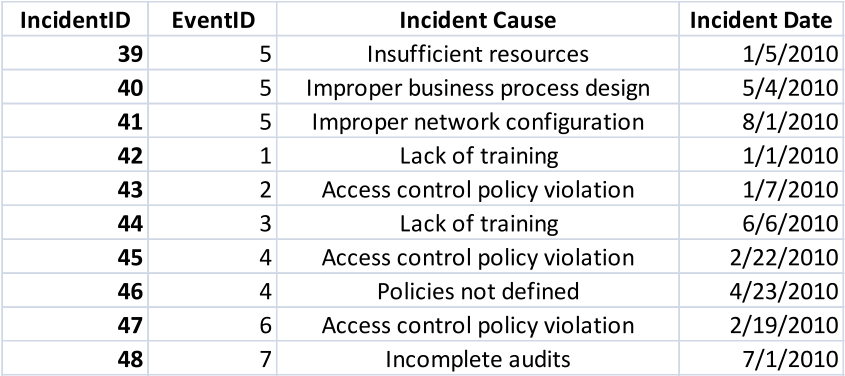
1. “Number of breaches” = 0.
2. Select all incidents in the incident knowledgebase where (“Start of Reporting Period” < “Date of Occurrence” <= “End of Reporting Period”) ***and*** (“Root Cause” = “Access Control Policy Violation”). Group incidents by “Reporting interval.”
3. For each selected incident, determine if any assets were affected.
4. For each asset affected, if asset was of type “information,” increment “Number of breaches.”

Example input data

The historical root causes for incidents that have occurred in the organization are as follows:

- policies not defined
- improper business process design
- improper network architecture
- lack of training
- incomplete audits
- insufficient resources
- access control policy violations (confidentiality, privacy)

The following table shows data needed for each incident, the 1:1 mapping between an incident and event(s) causing the incident (IncidentID:EventID), and the cause and date of the incident.



IncidentID	EventID	Incident Cause	Incident Date
39	5	Insufficient resources	1/5/2010
40	5	Improper business process design	5/4/2010
41	5	Improper network configuration	8/1/2010
42	1	Lack of training	1/1/2010
43	2	Access control policy violation	1/7/2010
44	3	Lack of training	6/6/2010
45	4	Access control policy violation	2/22/2010
46	4	Policies not defined	4/23/2010
47	6	Access control policy violation	2/19/2010
48	7	Incomplete audits	7/1/2010

The following table shows the data needed to connect each event to the affected asset, service, and/or organization unit.

EventMapping ID	EventID	AssetID	ServiceID	OrgUnitID
1	2	1	1	
2	2	6	1	
3	4			1
4	6	2		
5	6	3		
6	6	4		
7	6	5		
8	6			2

The following tables show the data needed to describe the asset type in an asset profile.

AssetID	AssetType	AssetSensitivity
1	Information	High
2	Facilities	High
3	Technology	High
4	Information	High
5	Information	Low
6	People	Medium

Example output data

Month	Number of Breaches
Jan	1
Feb	3
Mar	0
Apr	0
May	0
Jun	0
Jul	9
Aug	0
Sep	
Oct	
Nov	
Dec	

Plot *Months* as labels on the X axis, with *Count of Unauthorized Access* (breaches) on the Y axis.

Interpretation or Expected Value(s)	The bar chart shows the number of unauthorized accesses to information assets resulting from access control policy violations per month for the current year to date. Significant variation among months may indicate a security pattern worth investigating.

Measurement Template

Measure Name and ID	Unique name and identifier for the measure. For example: *Number of resilience requirements (RR_03).*
Goal	Statement of resilience goal. The goal should be connected to overall organizational strategic goals and critical success factors, organizational resilience goals, service resilience goals, and/or asset resilience goals.
Question(s)	What question(s) is the measure intending to answer? For example: *How many incidents occurred last quarter?* The question should relate to the goal.
Related Processes and Procedures	List of the names of the process and procedures where this measure is collected, including process and procedure measure IDs if applicable.
Visual Display	Graphical depiction of the measure. For example: trend over time, percentages, cumulative results, Pareto analysis, frequency diagrams, etc.
Data Input(s) **Data Elements** **Data Type**	All data elements (including measure name and ID, if applicable) and their type (base or derived) used as input for this measure.
Data Collection **How** **When/How Often** **By Whom**	How the data will be collected (process), when and how often the data will be collected (event driven, periodic), and who will collect the data (people, tool). Refer to forms or standards if needed.
Data Reporting **By/To Whom** **When/How Often**	The role that is responsible for reporting the measure. Identify for whom (what role) the report is intended. This may be an individual role or an organizational unit.
Data Storage **Where** **How** **Access Control**	Where the data is to be stored. Identify the storage media, procedures, and tools for configuration control. Specify how access to this data is controlled.
Stakeholders **Information Owner(s)** **Information Collector(s)** **Information Customer(s)**	Who will use this measure? How? What are the roles? Examples: asset owner, service owner, line of business manager, business continuity manager, steering group responsible for all aspects of resilience, including resilience measurement. Consider stakeholders external to the organization.
Algorithm or Formula	The algorithm or formula required to combine data elements to create input values for the measure. It may be very simple, such as input1/input2, or it may be much more complex. The relationship between the algorithm and the visual display should be explained as well.
Interpretation or Expected Value(s)	What different values of the measure mean. Make it clear how the measure answers the goal-related Question(s) above. Provide any important cautions about how the measure could be misinterpreted and actions to avoid misinterpretation. Provide guidance on how to interpret the measure and also what not to do with the measure. If the measure has a target value or range for success (meeting the goal), include that here.

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

[Allen 2011]

Allen, Julia, & Curtis, Pamela D. *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019). Software Engineering Institute, Carnegie Mellon University, September 2011. http://www.sei.cmu.edu/library/abstracts/reports/11tr019.cfm

[Brassard 2010]

Brassard, Michael & Ritter, Diane. *The Memory Jogger 2: A Pocket Guide of Tools for Continuous Improvement and Effective Planning,* 2nd edition. GOAL/QPC, 2010.

[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.

[Caralli 2007]

Caralli, Richard A., Stevens, James F., Young, Lisa R., & Wilson, William R. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process* (CMU/SEI-2007-TR-012). Software Engineering Institute, Carnegie Mellon University, 2007. http://www.sei.cmu.edu/library/abstracts/reports/07tr012.cfm

[Humphrey 1989]

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

[SPC 1996]

Software Productivity Consortium. *Improving the Software Process through Process Definition and Modeling*. International Thomson Computer Press, 1996.

[Stevens 2005]

Stevens, James F., Caralli, Richard A., & Willke, Bradford J. *Information Asset Profiling* (CMU/SEI-2005-TN-021). Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/library/abstracts/reports/05tn021.cfm

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY
(Leave Blank)

2. REPORT DATE
December 2011

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
Using Defined Processes as a Context for Resilience Measures

5. FUNDING NUMBERS
FA8721-05-C-0003

6. AUTHOR(S)
Julia H. Allen, Pamela D. Curtis, Linda Parker Gates

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2011-TN-029

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ESC/CAA
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125NO WARRANTY

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

The CERT® Resilient Enterprise Management (REM) team is researching operational resilience and the organizational processes that support it. The team's first report, *Measuring Operational Resilience Using the CERT® Resilience Management Model* (CMU/SEI-2010-TN-030), defined high-level objectives for managing an operational resilience management system, demonstrated how to derive meaningful measures from those objectives, and presented a template for defining resilience measures. The team's second report, *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019), suggested strategic measures for managing operational resilience and provided candidate measures for the 26 process areas of the CERT® Resilience Management Model, Version 1.1 (CERT®-RMM).

This technical note describes how implementation-level processes can provide the necessary context for identifying and defining measures of operational resilience. While CERT-RMM defines the commonly used or best practices for operational resilience—*what* an organization should do—organization-specific processes must be defined at the implementation level to describe *how* to perform those practices. Organizations can then identify and define measures within the context of their specific processes and constituent procedures. Organizations can use the measures to evaluate process performance and operational resilience and identify opportunities for improvement. This technical note provides examples and templates for defining processes and procedures and for defining related assets and measures.

14. SUBJECT TERMS
Resilience management, risk, measure, measurement, information security, risk management, operational risk management, process improvement, process definition, process implementation, resilience, operational resilience, CERT-RMM

15. NUMBER OF PAGES
56

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL