Software Engineering Institute

CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1

Kevin G. Partridge
Lisa R. Young

November 2011

TECHNICAL NOTE
CMU/SEI-2011-TN-028

CERT® Program

Unlimited distribution subject to the copyright.

http://www.sei.cmu.edu

Carnegie Mellon

Copyright 2012 Carnegie Mellon University.

This material is based upon work funded and supported by the United States Department of Homeland Security 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 sponsored by the United States Department of Defense.

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 United States Department of Homeland Security or the United States Department of Defense.

This report was prepared for the

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

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.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

® CERT, CERT Resilience Measurement Model, CERT-RMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

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

SEI markings v3.2 / 30 August 2011

Table of Contents

Abstract

The CERT® Resilience Management Model (CERT®-RMM) allows organizations to determine how their current practices support their desired levels of process maturity and improvement. This technical note maps CERT-RMM process areas to certain National Institute of Standards and Technology (NIST) special publications in the 800 series. It aligns the tactical practices suggested in the NIST publications to the process areas that describe management of operational resilience at a process level. This technical note is an extension of the *CERT-RMM Code of Practice Crosswalk, Commercial Version* (CMU/SEI-2011-TN-012).

1 Introduction

Organizations can use the CERT® Resilience Management Model (CERT®-RMM) V1.1 to determine how their current practices support their desired level of process maturity in the domains of security planning and management, business continuity and disaster recovery, and IT operations and service delivery. This technical note supplements and is a follow-on to the *CERT-RMM Code of Practice Crosswalk, Commercial Version* (CMU/SEI-2011-TN-012). This follow-on crosswalk connects CERT-RMM process areas to a focused set of National Institute of Standards and Technology (NIST) special publications in the 800 series.

This document helps to achieve a primary goal of CERT-RMM, which is to allow its adopters to continue to use preferred standards and codes of practice at a tactical level while maturing management and improvement of operational resilience at a process level. This document provides a reference for adopters of the model to determine how their current deployment of practices supports their desired level of process maturity and improvement.

The CERT-RMM process areas and the guidance within these NIST special publications are aligned only by subject matter. The materials often conflict, both in their level of detail and intended usage. Many of the NIST documents are very specific and provide direct operational guidance. These special publications are more prescriptive than the associated CERT-RMM specific practices. Where this is the case, this crosswalk aligns them according to their shared subject matter. It is not intended to provide a direct mapping of each step in the NIST best practices to each CERT-RMM specific practice and subpractice.

Some of the NIST special publications detail process requirements. These are much more closely and directly aligned with CERT-RMM goals and practices. In this case the alignment is obvious. However, a NIST special publication may not completely cover the goals or specific practices within a process area, but it may provide a component or subset of the related requirements at the goal or practice level. The crosswalk does not reflect the discontinuities at this level. It shows only the affinity between certain NIST 800-series special publications and CERT-RMM goals and practices according to their shared subject matter and focus.

This technical note shows the areas of overlap and redundancy between CERT-RMM process areas and the guidance in the NIST special publications, but it also shows the gaps that may affect the maturity of a practice. The CERT-RMM provides a reference model that allows organizations to make sense of their practices in a process context and improve processes and effectiveness. This crosswalk can help organizations align NIST practices to CERT-RMM process improvement goals.

1.1 CERT-RMM Description, Features, and Benefits

CERT-RMM V1.1 is a capability maturity model for managing operational resilience. It has two primary objectives:

® CERT® is a registered mark owned by Carnegie Mellon University.

- Establish the convergence of operational risk and resilience management activities (security planning and management, business continuity, IT operations, and service delivery) into a single model.
- Apply a process improvement approach to operational resilience management by defining and applying a capability scale expressed in increasing levels of process maturity.

CERT-RMM has the following features and benefits:

- provides a process definition, expressed in 26 process areas across four categories: enterprise management, engineering, operations, and process management
- focuses on the resilience of four essential operational assets: people, information, technology, and facilities
- includes processes and practices that define a scale of four capability levels for each process area: incomplete, performed, managed, and defined
- serves as a meta-model that easily coexists with and references common codes of practice, such as the NIST special publications 800 series, the International Organization for Standards (ISO) and International Electrotechnical Commission (IEC) 27000 series, COBIT, the British Standards Institution's BS 25999, and ISO 24762
- includes quantitative process measurements that can be used to ensure operational resilience processes are performing as intended
- facilitates an objective measurement of capability levels via a structured and repeatable appraisal methodology
- extends the process improvement and maturity pedigree of Capability Maturity Model Integration (CMMI®) to assurance, security, and service continuity activities

A copy of the current version of CERT-RMM can be obtained at http://www.cert.org/resilience/rmm.html.

1.2 CERT-RMM Structure in Relation to NIST Guidelines

CERT-RMM has several key components. The process area forms the major structural element in the model. Each process area has a series of descriptive components.

CERT-RMM refers to two types of practices: specific practices and subpractices. To make use of this crosswalk, it is important to understand the distinctions among these types of practices and the practices contained in common codes of practice.

1.2.1 Process Area

CERT-RMM comprises 26 process areas. Each process area describes a functional area of competency. In aggregate, these 26 process areas define the operational resilience management system. Process areas comprise goals, each achieved through specific practices, which are themselves broken down into subpractices.

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

Goals

Each process area has a set of goals. Goals are required elements of the process area, and they define its target accomplishments. An example of a goal from the Service Continuity process area is “SC:SG1 Prepare for Service Continuity.”

Generic goals are defined within individual process areas and pertain to elements that are relevant across all process areas. Their degree of achievement indicates a process’s level of institutionalization. Achievement of a generic goal is an indicator that the associated practices have been implemented across the process area. These goals ensure that the process area will be effective, repeatable, and lasting.

The crosswalk itself could be described as mapping strictly across Generic Goal 1, “Achieve Specific Goals.” This crosswalk is not intended to map NIST special publication guidelines across all generic goals or assert that a special publication helps an organization achieve any particular capability or maturity rating.

Specific Practices

Each process area goal has its own specific practices. Specific practices constitute a process area’s base practices, reflect its body of knowledge, and express what must be done. An example of a specific practice from the Service Continuity process area is “SC:SG1.SP1 Plan for Service Continuity,” which supports the goal “SC:SG1 Prepare for Service Continuity.”

Subpractices

Specific practices break down into subpractices. Subpractices are informative elements associated with each specific practice. These subpractices can often be related to specific process work products. Where specific practices focus on what must be done, subpractices focus on how it must be done. While not overly prescriptive or detailed, subpractices help the user determine how to satisfy the specific practices and achieve the goals of the process area. Each organization will have its own subpractices, either organically or by acquiring them from a code of practice.

Subpractices can be linked to the best practices and implementation guidance found in the NIST 800-series special publications. Subpractice instructions are usually broad, but many of the special publication guidelines can be definitive. For example, a subpractice may suggest that the user “set password standards and guidelines,” but a special publication may state that “passwords should be changed at 90-day intervals.”

2 NIST Publications

This section details the NIST 800-series special publications that are referenced in this document. The authors of this technical note chose these publications, which focus on IT security, for their utility within the Federal Information Security Management Act (FISMA) process as it is generally interpreted and because they cover a broad spectrum of FISMA requirements. Beginning with NIST SP 800-18, the publications provide guidance on security plan development. Each subsequent publication builds toward more specific guidance and requirements for a security program. The last three publications cover auxiliary topics impacting the risk management framework.

This section includes information on obtaining copies of each code of practice, which are freely available from the NIST website at http://csrc.nist.gov/publications/PubsSPs.html. NIST and the U.S. Department of Commerce retain all rights to and copyright of the NIST publications.

2.1 NIST SP 800-18

NIST Special Publication 800-18 Revision 1: Guide for Developing Security Plans for Federal Information Systems [NIST 2006] describes the development of security requirements and the implementation of controls based upon those requirements. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.

2.2 NIST SP 800-30

NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems [NIST 2002] covers risk calculation and management methodology. It is particularly oriented toward the management of risk in conjunction with an accreditation program. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

2.3 NIST SP 800-34

NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems [NIST 2010a] provides best practices for contingency plan development. It is a recommended guide for federal systems. The guidance provides a baseline of contingency plan practices. It also describes the interrelated, individual contingency plans and their roles in the system development lifecycle (SDLC). The publication discusses the integration of various requirements, including Federal Information Processing Standards (FIPS) Publication 199 and NIST Special Publication 800-53. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

2.4 NIST SP 800-37

NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST 2010b] provides guidance for federal information systems and the application of the Risk Management Framework. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

2.5 NIST SP 800-39

NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View [NIST 2011a] is the core document for integration of the NIST approach to risk management into a comprehensive Enterprise Risk Management (ERM) program. Developed in response to FISMA, SP 800-39 provides guidance on developing a comprehensive risk management program that includes all aspects of operations. Other, more focused NIST special publications support this guidance. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

2.6 NIST SP 800-53

NIST Special Publications 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations [NIST 2009] comprises a selection of security controls for executive federal agencies. These guidelines are pertinent to all system components that process federal information. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

2.7 NIST SP 800-53A

NIST Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans [NIST 2008a] details a process for assessing the effectiveness and appropriateness of the security controls deployed by a federal organization. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf.

2.8 NIST SP 800-55

NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security [NIST 2008b] provides guidance on the development of measures to describe the functioning of an organization’s security program, as well as guidance on the subsequent development of controls. The publication considers various mandates and requirements, including FISMA. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

2.9 NIST SP 800-60

NIST Special Publication 800-60 Volume I, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories [NIST 2008c] and *Volume II, Appendices* [NIST 2008d] provide guidelines for system owners mapping the sensitivity and criticality of their systems according to FISMA requirements. The current standard is version 1. They can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf and http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf.

2.10 NIST SP 800-61

NIST Standard Publication 800-61 Revision 1, Computer Security Incident Handling Guide [NIST 2008e] provides guidance for the appropriate handling of computer security incidents. The publication also contains guidance for implementing a tailored incident handling program. The current standard is version 1.2.1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

2.11 NIST SP 800-70

NIST Special Publication 800-70 Revision 2, National Checklist Program for IT Products—Guidelines for Checklist Users and Developers [NIST 2011b] is an index to the National Checklist Program's repository of checklists. It also provides guidance on the associated policies of the National Checklist Program. The current standard is version 1. It can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf.

2.12 NIST SP 800-137

NIST Special Publication 800-137 Initial Public Draft (IPD), Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST 2010c] comprises the NIST guidance for development and implementation of a continuous monitoring strategy. The guidance broadly focuses on awareness of threats and vulnerabilities, as well as the controls deployed against those vulnerabilities. The publication discusses a continuous strategy that balances risk, awareness, and response capability. The draft publication used for this crosswalk is no longer available and has been replaced by the final version 1.

3 CERT-RMM Crosswalk of NIST 800-Series Special Publications

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
ADM – Asset Definition and Management												
ADM:SG1 Establish Organizational Assets												
ADM:SG1.SP1 Inventory Assets				2.3		CM-8 PE-8 PL-2 PM-5 RA-2						
ADM:SG1.SP2 Establish a Common Understanding				2.3	2.6.2	PL-4			3.1			
ADM:SG1.SP3 Establish Ownership and Custodianship	1.7			2.3			3.1					2.4
ADM:SG2 Establish the Relationship Between Assets and Services												
ADM:SG2.SP1 Associate Assets with Services				2.1 2.3		PM-11 RA-2						
ADM:SG2.SP2 Analyze Asset-Service Dependencies												
ADM:SG3 Manage Assets												
ADM:SG3.SP1 Identify Change Criteria												2.1.1
ADM:SG3.SP2 Maintain Changes to Assets and Inventory												2.1.1
AM – Access Management												
AM:SG1 Manage and Control Access												
AM:SG1.SP1 Enable Access						AC-1 AC-2 AC-10 IA-1 IA-2 IA-8 MA-3 MA-4 MA-5 PE-1 PE-7 PE-16 PL-2 SA-7 SC-2 SI-9 SI-11						

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
AM:SG1.SP2 Manage Changes to Access Privileges						AC-2						
AM:SG1.SP3 Periodically Review and Maintain Access Privileges						AC-2						
AM:SG1.SP4 Correct Inconsistencies						AC-2						
COMM – Communications												
COMM:SG1 Prepare for Resilience Communications												
COMM:SG1.SP1 Identify Relevant Stakeholders										2.4.4		2.1
COMM:SG1.SP2 Identify Communications Requirements										2.3.4		2.1 3.1.1
COMM:SG1.SP3 Establish Communications Guidelines and Standards												3.1.1
COMM:SG2 Prepare for Communications Management												
COMM:SG2.SP1 Establish a Resilience Communications Plan							3.1					2.1.3
COMM:SG2.SP2 Establish a Resilience Communications Program												2.1.3
COMM:SG2.SP3 Identify and Assign Plan Staff							3.1					
COMM:SG3 Deliver Resilience Communications												
COMM:SG3.SP1 Identify Communications Methods and Channels			4.2.2									
COMM-3.SP2 Establish and Maintain Communications Infrastructure							3.1					
COMM:SG4 Improve Communications												
COMM:SG4.SP1 Assess Communications Effectiveness												
COMM:SG4.SP2 Improve Communications												
COMP – Compliance												
COMP:SG1 Prepare for Compliance Management												
COMP:SG1.SP1 Establish a Compliance Plan						CA-1						2.2
COMP:SG1.SP2 Establish a Compliance Program						AU-1						
COMP:SG1.SP3 Establish Compliance Guidelines and Standards						AU-3 AU-5						
COMP:SG2 Establish Compliance Obligations												
COMP:SG2.SP1 Identify Compliance Obligations						AU-2 SI-4						2.2
COMP:SG2.SP2 Analyze Obligations												
COMP:SG2.SP3 Establish Ownership for Meeting Obligations						AU-1						2.4
COMP:SG3 Demonstrate Satisfaction of Compliance Obligations												
COMP:SG3.SP1 Collect and Validate Compliance Data						AU-6 AU-11 PL-6						2.2 3.1.2
COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction						AU-7 AU-11 PL-6						3.1.2

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)										
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
COMP:SG3.SP3 Remediate Areas of Non-Compliance						PL-6						
COMP:SG4 Monitor Compliance Activities												
COMP:SG4.SP1 Evaluate Compliance Activities												
CTRL – Controls Management												
CTRL:SG1 Establish Control Objectives												
CTRL:SG1.SP1 Define Control Objectives			3.4	2.4			3.1 3.2.1					2.3 3.1.2
CTRL:SG2 Establish Controls												
CTRL:SG2.SP1 Define Controls			3.4	2.4 Task 2-1 Task 2-2		PM-7						3.1.2
CTRL: SG3 Analyze Controls												
CTRL:SG3.SP1 Analyze Controls				Task 2-1 Task 2-3 Task 3-1 App. G			3.2.1 3.2.2					2.2 3.1.1
CTRL:SG4 Assess Control Effectiveness												
CTRL:SG4.SP1 Assess Controls				Task 4-1 Task 4-2 Task 4-3 Task 4-4 Task 6-2 Task 6-3			3.3					2.2 3.1.2 3.5.1
EC – Environmental Control												
EC:SG1 Establish and Prioritize Facility Assets												
EC:SG1.SP1 Prioritize Facility Assets												
EC:SG1.SP2 Establish Resilience-Focused Facility Assets			3.4.3									
EC:SG2 Protect Facility Assets												
EC:SG2.SP1 Assign Resilience Requirements to Facility Assets			3.4.3			PE-3 PE-4 PE-6 PE-9 PE-13 PE-17 PE-18	3.1				3	
EC:SG2.SP2 Establish and Implement Controls			3.4.3			PE-7 PE-8 PE-16	3.1					
EC:SG3 Manage Facility Asset Risk												
EC:SG3.SP1 Identify and Assess Facility Asset Risk						PM-7						3.1.2

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)										
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
EC:SG3.SP2 Mitigate Facility Risks						PM-4 PM-7						3.1.2 3.6
EC:SG4 Control Operational Environment												
EC:SG4.SP1 Perform Facility Sustainability Planning			3.2			CP-6 CP-7 PE-10 PE-11 PE-12 PE-13 PM-11			3.2 4.6			
EC:SG4.SP2 Maintain Environmental Conditions						PE-10 PE-11 PE-12 PE-13 PE-14 PE-15						
EC:SG4.SP3 Manage Dependencies on Public Services												
EC:SG4.SP4 Manage Dependencies on Public Infrastructure						CP-8						
EC:SG4.SP5 Plan for Facility Retirement												
EF – Enterprise Focus												
EF:SG1 Establish Strategic Objectives												
EF:SG1.SP1 Establish Strategic Objectives						PM-7	3.1	5.2				2.1
EF:SG1.SP2 Establish Critical Success Factors			3.2.1			PM-7	3.1	1.4				
EF:SG1.SP3 Establish Organizational Services						PM-7 PM-11		5.5.2				
EF:SG2 Plan for Operational Resilience												
EF:SG2.SP1 Establish an Operational Resilience Management Plan						PL-2 PM-1 PM-4						
EF:SG2.SP2 Establish an Operational Resilience Management Program						PM-1 PM-4						
EF:SG3 Establish Sponsorship												
EF:SG3.SP1 Commit Funding for Operational Resilience Management						PM-3						
EF:SG3.SP2 Promote a Resilience-Aware Culture												
EF:SG3.SP3 Sponsor Resilience Standards and Policies						PL-1	3.1					
EF:SG4 Provide Resilience Oversight												
EF:SG4.SP1 Establish Resilience as a Governance Focus Area						CA-6 PL-1						
EF:SG4.SP2 Perform Resilience Oversight						PL-2						3.3.2

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
						PM-6						
EF:SG4.SP3 Establish Corrective Actions								6.3				
EXD – External Dependencies												
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												3.1.2
EXD:SG2.SP2 Mitigate Risks Due to External Dependencies												3.1.2 3.6
EXD:SG3 Establish Formal Relationships												
EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies						AC-20 SA-2 SA-12						
EXD:SG3.SP2 Establish Resilience Specifications for External Dependencies						SA-12 SA-13						
EXD:SG3.SP3 Evaluate and Select External Entities						SA-2 SA-3 SA-12						
EXD:SG3.SP4 Formalize Relationships						CA-3 SA-3 SA-4 SA-9 SA-11 SA-12 SA-13						
EXD:SG4 Manage External Entity Performance												
EXD:SG4.SP1 Monitor External Entity Performance						SA-3 SA-9 SA-12 SA-13						
EXD:SG4.SP2 Correct External Entity Performance						SA-3 SA-12						
FRM – Financial Resource Management												
FRM:SG1 Establish Financial Commitment												
FRM:SG1.SP1 Commit Funding for Operational Resilience Management						S						
FRM:SG1.SP2 Establish Structure to Support Financial Management												

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
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			3.4.5									
FRM:SG4 Account for Resilience Activities												
FRM:SG4.SP1 Track and Document Costs			3.4.5									
FRM:SG4.SP2 Perform Cost and Performance Analysis												2.3
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												2.3
HRM – Human Resource Management												
HRM:SG1 Establish Resource Needs												
HRM:SG1.SP1 Establish Baseline Competencies							3.1			2.4.2		
HRM:SG1.SP2 Inventory Skills and Identify Gaps										2.4.2		
HRM:SG1.SP3 Address Skill Deficiencies												
HRM:SG2 Manage Staff Acquisition												
HRM:SG2.SP1 Verify Suitability of Candidate Staff						PE-2	3.1					
HRM:SG2.SP2 Establish Terms and Conditions of Employment												
HRM:SG3 Manage Staff Performance												
HRM:SG3.SP1 Establish Resilience as a Job Responsibility							3.1					
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												
ID – Identity Management												
ID:SG1 Establish Identities												
ID:SG1.SP1 Create Identities						AC-5 AC-6 IA-2 IA-4 PE-2						

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
ID:SG1.SP2 Establish Identity Community						AC-5 AC-6 AC-22 IA-2 IA-4 PE-2						
ID:SG1.SP3 Assign Roles to Identities						AC-5 AC-6 IA-2 IA-4 PE-2						2.4
ID:SG2 Manage Identities												
ID:SG2.SP1 Monitor and Manage Identity Changes						AC-2						
ID:SG2.SP2 Periodically Review and Maintain Identities						AC-2						
ID:SG2.SP3 Correct Inconsistencies						AC-2						
ID:SG2.SP4 Deprovision Identities						AC-2						
IMC – Incident Management and Control												
IMC:SG1 Establish the Incident Management and Control Process												
IMC:SG1.SP1 Plan for Incident Management						AC-14 IR-4 IR-8				2.3		
IMC:SG1.SP2 Assign Staff to the Incident Management Plan						IR-2 IR-4 IR-8						
IMC:SG2 Detect Events												
IMC:SG2.SP1 Detect and Report Events			4.2			IR-4 IR-5 IR-6 PE-6 SI-5				3.2 4.3 5.3 6.3 7.3 8.2		2.1.3
IMC:SG2.SP2 Log and Track Events						IR-4 IR-5 IR-7						
IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence						IR-4 IR-5				3.2.5 3.3.2 3.4.2 3.4.3 4.4.2 5.4.2 6.4.2		

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
IMC:SG2.SP4 Analyze and Triage Events						IR-4				3.2.6 4.3 5.3 6.3 7.3 8.2		
IMC:SG3 Declare Incidents												
IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria			4.2.1			IR-4						3.3.4 3.1.1
IMC:SG3.SP2 Analyze Incidents			4.2.3			IR-4				3.2.4 4.3 5.3 6.3 7.3 8.2		
IMC:SG4 Respond to and Recover from Incidents												
IMC:SG4.SP1 Escalate Incidents						IR-4				3.2.4 3.2.7		
IMC:SG4.SP2 Develop Incident Response						IR-4				3 4 5 6 7 8		3.3.4
IMC:SG4.SP3 Communicate Incidents			4.2.2			IR-4				2.3.4 3.2.7		2.1.3
IMC:SG4.SP4 Close Incidents						IR-4				3.4		
IMC:SG5 Establish Incident Learning												
IMC:SG5.SP1 Perform Post-Incident Review						IR-4				3.4		
IMC:SG5.SP2 Integrate with the Problem Management Process						IR-4						3.3.4
IMC:SG5.SP3 Translate Experience to Strategy						IR-4						
KIM – Knowledge and Information Management												
KIM:SG1 Establish and Prioritize Information Assets												
KIM:SG1.SP1 Prioritize Information Assets												
KIM:SG1.SP2 Categorize Information Assets				2.1		AC-22			3.1.1 4			
KIM:SG2 Protect Information Assets												
KIM:SG2.SP1 Assign Resilience Requirements to Information Assets			3.4.1 3.4.2			AC-16 AC-21 SC-2	3.1		3.1.2 4			

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
						SI-12						
KIM:SG2.SP2 Establish and Implement Controls			3.4.1 3.4.2			AC-16 AC-21 MP-1 PE-5 SC-2 SI-12	3.1					
KIM:SG3 Manage Information Asset Risk												
KIM:SG3.SP1 Identify and Assess Information Asset Risk		3 5				PM-7						3.1.2
KIM:SG3.SP2 Mitigate Information Asset Risk		4				PM-4	PM-7					3.1.2 3.6
KIM:SG4 Manage Information Asset Confidentiality and Privacy												
KIM:SG4.SP1 Encrypt High-Value Information						MP-2 SC-8 SC-9 SC-11 SC-12 SC-13 SC-14 SC-17 SI-12						
KIM:SG4.SP2 Control Access to Information Assets						AU-13 IA-1 MP-2 MP-3 MP-4 MP-5 PL-5 SC-14 SI-11 SI-12						
KIM:SG4.SP3 Control Information Asset Disposition						MP-2 MP-3 MP-4 MP-5 MP-6 SC-14 SI-12						
KIM:SG5 Manage Information Asset Integrity												
KIM:SG5.SP1 Control Modification of Information Assets						SC-14						

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
KIM:SG5.SP2 Manage Information Asset Configuration						SC-14						2.1.1
KIM:SG5.SP3 Verify Validity of Information						SC-8 SC-14 SC-20 SC-21						
KIM:SG6 Manage Information Asset Availability												
KIM:SG6.SP1 Perform Information Duplication and Retention						CP-9				3.4.3		
KIM:SG6.SP2 Manage Organizational Knowledge												
MA – Measurement and Analysis												
MA:SG1 Align Measurement and Analysis Activities												
MA:SG1.SP1 Establish Measurement Objectives						PM-6	3.1 3.2.1 3.2.2 App. F	5.2 5.5 5.7 6.1		3.2.4		2.1.3 3.1.1 3.1.3 3.2
MA:SG1.SP2 Specify Measures							3.2.2 App. F	5.5				3.1.3 3.1.1 3.2
MA:SG1.SP3 Specify Data Collection and Storage Procedures								3.4.3 3.4.4 5.5		3.4.3		
MA:SG1.SP4 Specify Analysis Procedures							3.2.2 App. D App. F	5.7 6.2		3.2.4 4.3 5.3 6.3 7.3 8.2		2.1.2 3.1.1
MA:SG2 Provide Measurement Results												
MA:SG2.SP1 Collect Measurement Data							3.3	6.2				3.4
MA:SG2.SP2 Analyze Measurement Data								6.2				3.4 3.5
MA:SG2.SP3 Store Data and Results								3.4.3 6.2				3.4
MA:SG2.SP4 Communicate Results							App. G	6.2				2.1.3 3.4 3.5
MON – Monitoring												
MON:SG1 Establish and Maintain a Monitoring Program												
MON:SG1.SP1 Establish a Monitoring Program						CA-7 PM-6						2.1 2.3 3.1

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
												3.5 3.5.2
MON:SG1.SP2 Identify Stakeholders								5.1				2.4
MON:SG1.SP3 Establish Monitoring Requirements						CA-7 PM-6 SI-4		5.2			3	2.1 2.2 2.3 3.1 3.3
MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements												2.2 3.3
MON:SG2 Perform Monitoring												
MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure						RA-5						3.4
MON:SG2.SP2 Establish Collection Standards and Guidelines					3.4	RA-5		6.1				2.2 2.3 3.1
MON:SG2.SP3 Collect and Record Information					3.4	RA-5 SI-4		6.2				3.4
MON:SG2.SP4 Distribute Information					3.4	RA-5 SI-4						2.1.3 2.3 3.3 3.4 3.5.2
OPD – Organizational Process Definition												
OPD:SG1 Establish Organizational Process Assets												
OPD:SG1.SP1 Establish Standard Processes						PM-11	3.2 App. D App. E			3 4 5 6 7 8		3.1.1
OPD:SG1.SP2 Establish Tailoring Criteria and Guidelines							3.2 3.2.3 3.2.4					3.1.1
OPD:SG1.SP3 Establish the Organization’s Measurement Repository							3.2			3.4.2 3.4.3		3.1.1
OPD:SG1.SP4 Establish the Organization’s Process Asset Library												3.1.1
OPD:SG1.SP5 Establish Work Environment Standards												3.1.1
OPD:SG1.SP6 Establish Rules and Guidelines for Integrated Teams												3.1.1

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
OPF – Organizational Process Focus												
OPF:SG1 Determine Process Improvement Opportunities												
OPF:SG1.SP1 Establish Organizational Process Needs												3.1.1
OPF:SG1.SP2 Appraise the Organization’s Processes												2.3 3.7
OPF:SG1.SP3 Identify the Organization’s Process Improvements							3.2.5					2.3 3.7
OPF:SG2 Plan and Implement Process Actions												
OPF:SG2.SP1 Establish Process Action Plans							3.2.5					3.7
OPF:SG2.SP2 Implement Process Action Plans							3.2.5					3.7
OPF:SG3 Deploy Organizational Process Assets and Incorporate Experiences												
OPF:SG3.SP1 Deploy Organizational Process Assets												3.1.1
OPF:SG3.SP2 Deploy Standard Processes												3.1.1
OPF:SG3.SP3 Monitor the Implementation												3.7
OPF:SG3.SP4 Incorporate Experiences into Organizational Process Assets												
OTA – Organizational Training and Awareness												
OTA:SG1 Establish Awareness Program												
OTA:SG1.SP1 Establish Awareness Needs						AT-1						
OTA:SG1.SP2 Establish Awareness Plan						AT-1						
OTA:SG1.SP3 Establish Awareness Delivery Capability						AT-1						
OTA:SG2 Conduct Awareness Activities												
OTA:SG2.SP1 Perform Awareness Activities						AT-2				3.2.3		3.1.1
OTA:SG2.SP2 Establish Awareness Records						AT-4						
OTA:SG2.SP3 Assess Awareness Program Effectiveness												
OTA:SG3 Establish Training Capability												
OTA:SG3.SP1 Establish Training Needs			3.5			AT-1						
OTA:SG3.SP2 Establish Training Plan			3.5.1			AT-1						
OTA:SG3.SP3 Establish Training Capability						AT-1						
OTA:SG4 Conduct Training												
OTA:SG4.SP1 Deliver Training						AT-3						
OTA:SG4.SP2 Establish Training Records						AT-4						
OTA:SG4.SP3 Assess Training Effectiveness												
PM – People Management												
PM:SG1 Establish Vital Staff												
PM:SG1.SP1 Identify Vital Staff										2.4.3		
PM:SG2 Manage Risks Associated with Staff Availability												
PM:SG2.SP1 Identify and Assess Staff Risk						PM-7				2.4.3		
PM:SG2.SP2 Mitigate Staff Risk						PM-4				2.4.3		

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
						PM-7						
PM:SG3 Manage the Availability of Staff												
PM:SG3.SP1 Establish Redundancy for Vital Staff												
PM:SG3.SP2 Perform Succession Planning						PM-11						
PM:SG3.SP3 Prepare for Redeployment												
PM:SG3.SP4 Plan to Support Staff During Disruptive Events						PM-11						
PM:SG3.SP5 Plan for Return-to-Work Considerations						PM-11						
RISK – Risk Management												
RISK:SG1 Prepare for Risk Management												
RISK:SG1.SP1 Determine Risk Sources and Categories		3.2		2.1	3.2	RA-2						2.1.3
RISK:SG1.SP2 Establish an Operational Risk Management Strategy		2		2.1	2.1 2.2 2.6	PM-9	3.1			3.1.2 4.2.2 5.2.2 6.2.2 7.2.2		2.1.3 2.2 3.1.1
RISK:SG2 Establish Risk Parameters and Focus												
RISK:SG2.SP1 Define Risk Parameters					2.2	CA-6 PM-9 RA-3	3.1					2.2 3.1.1
RISK:SG2.SP2 Establish Risk Measurement Criteria		3.7			3.2	PM-9 RA-3	3.1	5.5				2.1.3 3.1.1
RISK:SG3 Identify Risk												
RISK:SG3.SP1 Identify Asset-Level Risks		3			3.2	CA-2 PL-5 PL-6 PM-9 RA-3			4.2 4.3 4.4 4.5			2.2
RISK:SG3.SP2 Identify Service-Level Risks		3			3.2	PL-5 PL-6 PM-9 RA-3						2.2
RISK:SG4 Analyze Risk												
RISK:SG4.SP1 Evaluate Risk		3 5				PL-5 PL-6 PM-9 RA-3						
RISK:SG4.SP2 Categorize and Prioritize Risk		3		2.1		PL-5 PL-6 PM-9 RA-3						3.1.1

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
RISK:SG4.SP3 Assign Risk Disposition						PL-5 PL-6 PM-9 RA-3						2.2 3.1.1 3.1.2
RISK:SG5 Mitigate and Control Risk												
RISK:SG5.SP1 Develop Risk Mitigation Plans		4			2.2	CA-5 PM-4 PM-9 RA-3						3.1.2 3.6
RISK:SG5.SP2 Implement Risk Strategies					2.2	PM-9 RA-3						2.2 3.1.1 3.6
RISK:SG6 Use Risk Information to Manage Resilience												
RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services						PM-9						2.2 3.1.1
RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services						PM-9						2.2 3.1.1
RRD – Resilience Requirements Development												
RRD:SG1 Identify Enterprise Requirements												
RRD:SG1.SP1 Establish Enterprise Resilience Requirements						PM-7	2.3					
RRD:SG2 Develop Service Requirements												
RRD:SG2.SP1 Establish Asset Resilience Requirements	1.8 2					SA-2 SA-13	2.3 3.1 3.2.1		4.6		3	
RRD:SG2.SP2 Assign Enterprise Resilience Requirements to Services	2.5.1 2.5.3					PM-7						
RRD:SG3 Analyze and Validate Requirements												
RRD:SG3.SP1 Establish a Definition of Required Functionality	3.9											2.1
RRD:SG3.SP2 Analyze Resilience Requirements						SA-13	3.1					
RRD:SG3.SP3 Validate Resilience Requirements						SA-13	3.1				4	
RRM – Resilience Requirements Management												
RRM:SG1 Manage Requirements												
RRM:SG1.SP1 Obtain an Understanding of Resilience Requirements	2.5					PM-7	3.1				4	
RRM:SG1.SP2 Obtain Commitment to Resilience Requirements	3					SA-2						
RRM:SG1.SP3 Manage Resilience Requirements Changes	3								4.6			2.1.1 2.1.2 3.6 3.7
RRM:SG1.SP4 Maintain Traceability of Resilience Requirements	3											

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
RRM:SG1.SP5 Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements						PM-7	3.1					
RTSE – Resilient Technical Solution Management												
RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development												
RTSE:SG1.SP1 Identify General Guidelines				2.2		SA-4					3	
RTSE:SG1.SP2 Identify Requirements Guidelines						SA-4 SA-13					3	
RTSE:SG1.SP3 Identify Architecture and Design Guidelines						SA-4					3	
RTSE:SG1.SP4 Identify Implementation Guidelines						SA-4 SA-11						
RTSE:SG1.SP5 Identify Assembly and Integration Guidelines						SA-4 SA-11						
RTSE:SG2 Develop Resilient Technical Solution Development Plans												
RTSE:SG2.SP1 Select and Tailor Guidelines	2.5					SA-12 SA-14					4	
RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process				2.2		PM-7 SA-3 SA-12 SA-14						
RTSE:SG3 Execute the Plan												
RTSE:SG3.SP1 Monitor Execution of the Development Plan						SA-12 SA-14						
RTSE:SG3.SP2 Release Resilient Technical Solutions into Production						SA-12 SA-14						2.2
SC – Service Continuity												
SC:SG1 Prepare for Service Continuity												
SC:SG1.SP1 Plan for Service Continuity			3.1 3.4			CP-1 PM-11						
SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity			3.1 4									
SC:SG2 Identify and Prioritize High-Value Services												
SC:SG2.SP1 Identify the Organization's High-Value Services			3.2			CP-2						
SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies			3.2			AT-5 PM-8 SC-8						
SC:SG2.SP3 Identify Vital Organizational Records and Databases			3.2			SC-9						
SC:SG3 Develop Service Continuity Plans												
SC:SG3.SP1 Identify Plans to Be Developed						CP-10 PM-11						
SC:SG3.SP2 Develop and Document Service Continuity Plans			3.4			CP-2						

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
						PL-6						
SC:SG3.SP3 Assign Staff to Service Continuity Plans			3.4.6			CP-2						
SC:SG3.SP4 Store and Secure Service Continuity Plans												
SC:SG3.SP5 Develop Service Continuity Plan Training			3.5.2			CP-3						
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						PL-6						
SC:SG5.SP2 Develop and Document Test Plans						CP-4 PL-6						
SC:SG5.SP3 Exercise Plans			3.5.3			CP-3 CP-4 PL-6						
SC:SG5.SP4 Evaluate Plan Test Results						CP-4 PL-6						
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			3.6			CP-2						
TM – Technology Management												
TM:SG1 Establish and Prioritize Technology Assets												
TM:SG1.SP1 Prioritize Technology Assets			3.2.3			PL-2 PM-5 SA-14						
TM:SG1.SP2 Establish Resilience-Focused Technology Assets						PM-5 SA-14						
TM:SG2 Protect Technology Assets												
TM:SG2.SP1 Assign Resilience Requirements to Technology Assets	3.2					AC-14 CM-6 CM-7 PL-2 SA-13 SC-2	3.1		3.1 4		3	
TM:SG2.SP2 Establish and Implement Controls	2.5 3.13 3.14		3.3			AC-14 AU-3 AU-7 AU-8	3.1					

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
						AU-9 AU-10 AU-12 AU-14 CM-7 PE-5 PL-2 PL-6 PM-7						
TM:SG3 Manage Technology Asset Risk												
TM:SG3.SP1 Identify and Assess Technology Asset Risk		3 5				CM-4 PL-6 PM-7 PM-10						
TM:SG3.SP2 Mitigate Technology Risk		4	3.3			PM-4 PM-7 PM-10						3.1.2 3.6
TM:SG4 Manage Technology Asset Integrity												
TM:SG4.SP1 Control Access to Technology Assets	2.5 3.13 3.14					AC-3 AC-4 AC-7 AC-8 AC-9 AC-11 AC-17 AC-18 AC-19 CM-5 IA-3 IA-5 IA-6 IA-7 IA-8 MA-1 MA-3 MA-4 MA-5						
TM:SG4.SP2 Perform Configuration Management	3.16					AC-19 CM-1 CM-2 CM-3 CM-6						2.1.1

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
						CM-9 SA-5 SA-10 SI-2						2.1.2
TM:SG4.SP3 Perform Change Control and Management	3.16					CM-3 CM-4 SA-10 SI-5						2.1.1
TM:SG4.SP4 Perform Release Management						IA-2 PM-10						2.2
TM:SG5 Manage Technology Asset Availability												
TM:SG5.SP1 Perform Planning to Sustain Technology Assets			3.4.4			PE-11 PL-6 PM-11 SI-6 SI-13						
TM:SG5.SP2 Manage Technology Asset Maintenance						AU-5 MA-2 MA-4 MA-6 PL-6						
TM:SG5.SP3 Manage Technology Capacity						AU-4 SI-6						
TM:SG5.SP4 Manage Technology Interoperability	3.11											
VAR – Vulnerability Analysis and Resolution												
VAR:SG1 Prepare for Vulnerability Analysis and Resolution												
VAR:SG1.SP1 Establish Scope							2.2 2.3 3.2 App. D App. E				3	
VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy		3.3					2.2 2.3 2.4 3.2 App. D App. E App. F			4.2.2 5.2.2 6.2.2 7.2.2		3.1.1
VAR:SG2 Identify and Analyze Vulnerabilities												
VAR:SG2.SP1 Identify Sources of Vulnerability Information		3.3.1				RA-5				3.1.2 3.2.4		2.1.3

CERT-RMM V1.1 Process Areas, Goals, and Specific Practices	NIST Special Publication Section Numbers (Control Numbers for 800-53 Rev. 3)											
	800-18 Rev.1	800-30	800-34 Rev. 1	800-37 Rev. 1	800-39	800-53 Rev. 3	800-53A Rev. 1	800-55 Rev. 1	800-60 Vol. 1 Rev.1	800-61 Rev. 1	800-70 Rev. 2	800-137 (IPD)
VAR:SG2.SP2 Discover Vulnerabilities		3.3.2	3.3			RA-5 SA-10 SA-11 SI-2 SI-3						3.1.2
VAR:SG2.SP3 Analyze Vulnerabilities		3.4 3.6				RA-5 SA-10 SA-11 SI-2 SI-3						2.1.2
VAR:SG3 Manage Exposure to Vulnerabilities												
VAR:SG3.SP1 Manage Exposure to Vulnerabilities			3.3			RA-5 SA-10 SA-11 SI-2 SI-3						
VAR:SG4 Identify Root Causes												
VAR:SG4.SP1 Perform Root-Cause Analysis						RA-5 SA-11 SI-2				3.4		

References

URLs valid at time of reference.

[NIST 2002]

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems*. NIST, 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[NIST 2006]

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems*. NIST, 2006. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

[NIST 2008a]

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.* NIST, 2008. http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf

[NIST 2008b]

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security*. NIST, 2008. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

[NIST 2008c]

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-60 Revision I, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*. NIST, 2008. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

[NIST 2008d]

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-60 Revision I, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.* NIST, 2008. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf

[NIST 2008e]

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-61 Revision 1, Computer Security Incident Handling Guide*. NIST, 2008. http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

[NIST 2009]

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information*

Systems and Organizations. NIST, 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[NIST 2010a]
National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.* NIST, 2010. http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

[NIST 2010b]
National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* NIST, 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[NIST 2010c]
National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-137 Initial Public Draft (IPD), Information Security Continuous Monitoring for Federal Information Systems and Organizations.* NIST, 2010.

[NIST 2011a]
National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.* NIST, 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[NIST 2011b]
National Institute of Standards and Technology (NIST). U.S. Department of Commerce. *NIST Special Publication 800-70 Revision 2, National Checklist Program for IT Products—Guidelines for Checklist Users and Developers.* NIST, 2011. http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf

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**
November 2011

3. **REPORT TYPE AND DATES COVERED**
Final

4. **TITLE AND SUBTITLE**
CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1

5. **FUNDING NUMBERS**
FA8721-05-C-0003

6. **AUTHOR(S)**
Kevin G. Partridge
Lisa R. Young

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-028

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

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® Resilience Management Model (CERT®-RMM) allows organizations to determine how their current practices support their desired levels of process maturity and improvement. This technical note maps CERT-RMM process areas to certain National Institute of Standards and Technology (NIST) special publications in the 800 series. It aligns the tactical practices suggested in the NIST publications to the process areas that describe management of operational resilience at a process level. This technical note is an extension of the *CERT-RMM Code of Practice Crosswalk, Commercial Version* (CMU/SEI-2011-TN-012).

14. **SUBJECT TERMS**
NIST, Special Publication, Security, Model, RMM, Resilience, Risk

15. **NUMBER OF PAGES**
34

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