Software Engineering Institute

# CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 2

Kevin G. Partridge
Mary E. Popeck
Lisa R. Young

**June 2014**

**TECHNICAL NOTE**
CMU/SEI-2014-TN-004

**CERT® Division**

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported 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.



This report was prepared for the

SEI Administrative Agent

AFLCMC/PZM

20 Schilling Circle, Bldg 1305, 3rd floor

Hanscom AFB, MA 01731-2125



DM-0001302

# 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) and an update to the *CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1* (CMU/SEI-2011-TN-028).

# 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 Resilience Management Model (RMM) v1.1: Code of Practice Crosswalk Commercial Version 1.1* [Partridge 2011a]. 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. Additionally, this technical note updates *CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1* [Partridge 2011b] with new mappings to the CERT-RMM based on the latest versions of NIST SP 800-30, NIST SP 800-53, NIST SP 800-61, and NIST SP 800-137.

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.

Some of the NIST special publications detail process requirements. These much more closely and directly align with CERT-RMM goals and practices. In this case the alignment is obvious. 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; 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.

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

## 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:

- 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:

- defines processes, 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 version 1.0 of CERT-RMM can be obtained at http://www.cert.org/resilience/products-services/cert-rmm/cert-rmm-model.cfm.

## 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

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

system. Process areas comprise goals, each achieved through specific practices, which are themselves broken down into subpractices.

## 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 that it either develops organically or acquires 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 the publications 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 Rev. 1

*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 standard used in this mapping can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.

## 2.2 NIST SP 800-30 Rev. 1

*NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments* [NIST 2012a] covers risk calculation and management methodology. It is particularly oriented toward the management of risk in conjunction with an accreditation program. The standard used in this mapping can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

## 2.3 NIST SP 800-34 Rev. 1

*NIST Special Publication 800-34 Revision 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 SP 800-53. The standard used in this mapping 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 Rev. 1

*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 standard used in this mapping 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 standard used in this mapping can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

## 2.6 NIST SP 800-53 Rev. 4

*NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013] comprises a selection of security and privacy controls for executive federal agencies. These guidelines are pertinent to all system components that process federal information. The standard used in this mapping can be downloaded at http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Appendix J, Privacy Control Catalog, is a new addition to NIST 800-53. Its privacy controls have been mapped to CERT-RMM as a special type of controls for handling and protecting an organization's critical information. Though personally identifiable information (PII) is most critical to individuals, organizations may suffer legal penalties and harm to their reputation if they do not properly implement privacy controls. As a result, PII may be thought of as critical information with unique requirements and, if improperly handled, legal ramifications.

## 2.7 NIST SP 800-53A Rev. 1

*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 2010c] details a process for assessing the effectiveness and appropriateness of the security controls deployed by a federal organization. The standard used in this mapping can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

## 2.8 NIST SP 800-55 Rev. 1

*NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security* [NIST 2008a] 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 standard used in this mapping can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

## 2.9 NIST SP 800-60 Rev. 1

*NIST Special Publication 800-60 Volume I Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories* [NIST 2008b] and *Volume II, Appendices* [NIST

2008c] provide guidelines for system owners mapping the sensitivity and criticality of their systems according to FISMA requirements. The standards used in this mapping 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 Rev. 2

*NIST Standard Publication 800-61 Revision 2, Computer Security Incident Handling Guide* [NIST 2012b] provides guidance for the appropriate handling of computer security incidents. The publication also contains guidance for implementing a tailored incident handling program. The standard used in this mapping can be downloaded at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

## 2.11 NIST SP 800-70 Rev. 2

*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 standard used in this mapping 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, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* [NIST 2011c] 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 standard used in this mapping can be downloaded at http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

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

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| ADM – Asset Definition and Management | | |
| *ADM:SG1 Establish Organizational Assets* | | |
| ADM:SG1.SP1 Inventory Assets | 37R1 | 2.3 |
| | 53R4 | CM-8, PE-8, PE-20, PM-5, RA-2, SA-19, SC-38 |
| ADM:SG1.SP2 Establish a Common Understanding | 37R1 | 2.3 |
| | 39 | 2.6.2 |
| | 60V1R1 | 3.1 |
| ADM:SG1.SP3 Establish Ownership and Custodianship | 18R1 | 1.7 |
| | 37R1 | 2.3 |
| | 53AR1 | 3.1 |
| *ADM:SG2 Establish the Relationship Between Assets and Services* | | |
| ADM:SG2.SP1 Associate Assets with Services | 37R1 | 2.1, 2.3 |
| | 53R4 | PM-11, RA-2, SE-1 |
| ADM:SG2.SP2 Analyze Asset-Service Dependencies | | |
| *ADM:SG3 Manage Assets* | | |
| ADM:SG3.SP1 Identify Change Criteria | 53R4 | SA-22 |
| ADM:SG3.SP2 Maintain Changes to Assets and Inventory | 53R4 | PE-20, SE-1 |
| AM – Access Management | | |
| *AM:SG1 Manage and Control Access* | | |
| AM:SG1.SP1 Enable Access | 53R4 | AC-1, AC-2, AC-3, AC-5, AC-6, AC-10, AC-12, AC-24, AC-25, AR-3, CM-11, IA-1, IA-2, IA-8, IP-2, MA-3, MA-4, MA-5, MP-2, PE-1, PE-2, PE-3, PE-16, PL-2, PL-4, SA-21, SC-2, SI-11 |
| AM:SG1.SP2 Manage Changes to Access Privileges | 53R4 | AC-2 |
| AM:SG1.SP3 Periodically Review and Maintain Access Privileges | 53R4 | AC-2 |
| AM:SG1.SP4 Correct Inconsistencies | 53R4 | AC-2 |
| COMM – Communications | | |
| *COMM:SG1 Prepare for Resilience Communications* | | |
| COMM:SG1.SP1 Identify Relevant Stakeholders | | |
| COMM:SG1.SP2 Identify Communications Requirements | | |
| COMM:SG1.SP3 Establish Communications Guidelines and Standards | 53R4 | IP-3 |
| *COMM:SG2 Prepare for Communications Management* | | |
| COMM:SG2.SP1 Establish a Resilience Communications Plan | 53AR1 | 3.1 |
| COMM:SG2.SP2 Establish a Resilience Communications Program | 53R4 | PM-16, TR-1, TR-2, TR-3 |
| COMM:SG2.SP3 Identify and Assign Plan Staff | 53AR1 | 3.1 |
| *COMM:SG3 Deliver Resilience Communications* | | |
| COMM:SG3.SP1 Identify Communications Methods and Channels | 34R1 | 4.2.2 |
| | 53R4 | CA-9, PM-15, SC-37, SI-5 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| COMM:SG3.SP2 Establish and Maintain Communications Infrastructure | 53R4 | SI-5 |
| | 53AR1 | 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 | 53R4 | CA-1 |
| COMP:SG1.SP2 Establish a Compliance Program | 53R4 | AU-1 |
| COMP:SG1.SP3 Establish Compliance Guidelines and Standards | 53R4 | AU-3, AU-5, UL-2 |
| *COMP:SG2 Establish Compliance Obligations* | | |
| COMP:SG2.SP1 Identify Compliance Obligations | 53R4 | AP-1, AP-2, AR-1, AU-2, CM-10, DM-3, SI-4 |
| COMP:SG2.SP2 Analyze Obligations | 53R4 | CM-10 |
| COMP:SG2.SP3 Establish Ownership for Meeting Obligations | 53R4 | AU-1, DI-2 |
| *COMP:SG3 Demonstrate Satisfaction of Compliance Obligations* | | |
| COMP:SG3.SP1 Collect and Validate Compliance Data | 53R4 | AR-4, AR-8, AU-3, AU-6, AU-11, AU-16, CM-10, IP-2, UL-1, UL-2 |
| COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction | 53R4 | AR-6, AU-7, AU-11, CM-11 |
| COMP:SG3.SP3 Remediate Areas of Non-Compliance | 53R4 | AR-4 |
| *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 | 34R1 | 3.4 |
| | 37R1 | 2.4 |
| | 53AR1 | 3.1, 3.2.1 |
| | 137 | 2.1, 3.1.3 |
| *CTRL:SG2 Establish Controls* | | |
| CTRL:SG2.SP1 Define Controls | 34R1 | 3.4 |
| | 37R1 | 2.4, Task 2-1, Task 2-2 |
| | 53R4 | AU-15, PM-7, SA-15 |
| | 137 | 2.1.2 |
| *CTRL: SG3 Analyze Controls* | | |
| CTRL:SG3.SP1 Analyze Controls | 37R1 | Task 2-1, Task 2-3, Task 3-1, App. G |
| | 53AR1 | 3.2.1, 3.2.2 |
| | 137 | 2.1.2, 2.1.3, 3.1.2, 3.2.1, 3.2.2, 3.3, 3.4.1, 3.4.2, 3.5, 3.6 |
| *CTRL:SG4 Assess Control Effectiveness* | | |
| CTRL:SG4.SP1 Assess Controls | 37R1 | Task 4-1, Task 4-2, Task 4-3, Task 4-4, Task 6-2, Task 6-3 |
| | 53AR1 | 3.3 |
| | 137 | 2.1.3, 2.2, 3.1.2, 3.1.3, 3.2.2, 3.3, 3.4.2, 3.5, 3.6 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| EC – Environmental Control | | |
| *EC:SG1 Establish and Prioritize Facility Assets* | | |
| EC:SG1.SP1 Prioritize Facility Assets | | |
| EC:SG1.SP2 Establish Resilience-Focused Facility Assets | 34R1 | 3.4.3 |
| | 53R4 | SC-44 |
| *EC:SG2 Protect Facility Assets* | | |
| EC:SG2.SP1 Assign Resilience Requirements to Facility Assets | 34R1 | 3.4.3 |
| | 53R4 | PE-3, PE-4, PE-6, PE-9, PE-13, PE-17, PE-18 |
| | 53AR1 | 3.1 |
| | 70R2 | 3 |
| EC:SG2.SP2 Establish and Implement Controls | 34R1 | 3.4.3 |
| | 53R4 | CP-12, CP-13, PE-2, PE-3, PE-8, PE-16, SC-40 |
| | 53AR1 | 3.1 |
| *EC:SG3 Manage Facility Asset Risk* | | |
| EC:SG3.SP1 Identify and Assess Facility Asset Risk | 53R4 | PM-7 |
| EC:SG3.SP2 Mitigate Facility Risks | 53R4 | PM-4, PM-7, SA-22, SC-36, SC-37, SC-38 |
| *EC:SG4 Control Operational Environment* | | |
| EC:SG4.SP1 Perform Facility Sustainability Planning | 34R1 | 3.2 |
| | 53R4 | CP-6, CP-7, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PM-11 |
| | 60V1R1 | 3.2, 4.6 |
| EC:SG4.SP2 Maintain Environmental Conditions | 53R4 | 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 | 53R4 | CP-8 |
| EC:SG4.SP5 Plan for Facility Retirement | | |
| EF – Enterprise Focus | | |
| *EF:SG1 Establish Strategic Objectives* | | |
| EF:SG1.SP1 Establish Strategic Objectives | 53R4 | AP-2, PM-7 |
| | 53AR1 | 3.1 |
| | 55R1 | 5.2 |
| EF:SG1.SP2 Establish Critical Success Factors | 34R1 | 3.2.1 |
| | 53R4 | IP-1, PM-7 |
| | 53AR1 | 3.1 |
| | 55R1 | 1.4 |
| EF:SG1.SP3 Establish Organizational Services | 53R4 | PM-7, PM-11 |
| | 55R1 | 5.5.2 |
| *EF:SG2 Plan for Operational Resilience* | | |
| EF:SG2.SP1 Establish an Operational Resilience Management Plan | 53R4 | AR-1, IP-2, PL-2, PL-7, PL-8, PM-1, PM-4, PM-8 |
| EF:SG2.SP2 Establish an Operational Resilience Management Program | 53R4 | AR-1, IP-2, PL-9, PM-1, PM-4, PM-13 |
| *EF:SG3 Establish Sponsorship* | | |
| EF:SG3.SP1 Commit Funding for Operational Resilience Management | 53R4 | PM-3 |
| EF:SG3.SP2 Promote a Resilience-Aware Culture | | |
| EF:SG3.SP3 Sponsor Resilience Standards and Policies | 53R4 | PL-1 |
| | 53AR1 | 3.1 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| *EF:SG4 Provide Resilience Oversight* | | |
| EF:SG4.SP1 Establish Resilience as a Governance Focus Area | 53R4 | CA-6, PL-1 |
| EF:SG4.SP2 Perform Resilience Oversight | 53R4 | PM-6 |
| EF:SG4.SP3 Establish Corrective Actions | 55R1 | 6.3 |
| EXD – External Dependencies | | |
| *EXD:SG1 Identify and Prioritize External Dependencies* | | |
| EXD:SG1.SP1 Identify External Dependencies | 53R4 | PL-8 |
| EXD:SG1.SP2 Prioritize External Dependencies | | |
| *EXD:SG2 Manage Risks Due to External Dependencies* | | |
| EXD:SG2.SP1 Identify and Assess Risks Due to External Dependencies | | |
| EXD:SG2.SP2 Mitigate Risks Due to External Dependencies | 53R4 | SA-21, SC-38 |
| *EXD:SG3 Establish Formal Relationships* | | |
| EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies | 53R4 | AC-20, AR-3, SA-2, SA-12, UL-2 |
| EXD:SG3.SP2 Establish Resilience Specifications for External Dependencies | 53R4 | SA-12, SA-13 |
| EXD:SG3.SP3 Evaluate and Select External Entities | 53R4 | SA-2, SA-3, SA-12 |
| EXD:SG3.SP4 Formalize Relationships | 53R4 | AU-16, CA-3, DI-2, 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 | 53R4 | AR-4, SA-3, SA-9, SA-12, SA-13 |
| EXD:SG4.SP2 Correct External Entity Performance | 53R4 | SA-3, SA-12 |
| FRM – Financial Resource Management | | |
| *FRM:SG1 Establish Financial Commitment* | | |
| FRM:SG1.SP1 Commit Funding for Operational Resilience Management | | |
| FRM:SG1.SP2 Establish Structure to Support Financial Management | | |
| *FRM:SG2 Perform Financial Planning* | | |
| FRM:SG2.SP1 Define Funding Needs | | |
| FRM:SG2.SP2 Establish Resilience Budgets | | |
| FRM:SG2.SP3 Resolve Funding Gaps | | |
| *FRM:SG3 Fund Resilience Activities* | | |
| FRM:SG3.SP1 Fund Resilience Activities | 34R1 | 3.4.5 |
| *FRM:SG4 Account for Resilience Activities* | | |
| FRM:SG4.SP1 Track and Document Costs | 34R1 | 3.4.5 |
| FRM:SG4.SP2 Perform Cost and Performance Analysis | | |
| *FRM:SG5 Optimize Resilience Expenditures and Investments* | | |
| FRM:SG5.SP1 Optimize Resilience Expenditures | | |
| FRM:SG5.SP2 Determine Return on Resilience Investments | | |
| FRM:SG5.SP3 Identify Cost Recovery Opportunities | | |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| HRM – Human Resource Management | | |
| *HRM:SG1 Establish Resource Needs* | | |
| HRM:SG1.SP1 Establish Baseline Competencies | 53AR1 | 3.1 |
| HRM:SG1.SP2 Inventory Skills and Identify Gaps | | |
| HRM:SG1.SP3 Address Skill Deficiencies | | |
| *HRM:SG2 Manage Staff Acquisition* | | |
| HRM:SG2.SP1 Verify Suitability of Candidate Staff | 53R4 | PE-2 |
| | 53AR1 | 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 | 53AR1 | 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 | 53R4 | AC-5, AC-6, IA-2, IA-4, IA-9, PE-2 |
| ID:SG1.SP2 Establish Identity Community | 53R4 | AC-5, AC-6, AC-22, IA-2, IA-4, PE-2 |
| ID:SG1.SP3 Assign Roles to Identities | 53R4 | AC-5, AC-6, IA-1, IA-2, IA-4, PE-2 |
| *ID:SG2 Manage Identities* | | |
| ID:SG2.SP1 Monitor and Manage Identity Changes | 53R4 | AC-2, IA-11 |
| ID:SG2.SP2 Periodically Review and Maintain Identities | 53R4 | AC-2, IA-11 |
| ID:SG2.SP3 Correct Inconsistencies | 53R4 | AC-2 |
| ID:SG2.SP4 Deprovision Identities | 53R4 | AC-2 |
| IMC – Incident Management and Control | | |
| *IMC:SG1 Establish the Incident Management and Control Process* | | |
| IMC:SG1.SP1 Plan for Incident Management | 53R4 | AC-14, IR-4, IR-8, PM-12, SA-15, SE-2 |
| | 61R2 | 2, 2.3, 2.3.2 |
| IMC:SG1.SP2 Assign Staff to the Incident Management Plan | 53R4 | IR-4, IR-8, IR-10 |
| | 61R2 | 2.4, 2.4.2, 2.4.3, 2.4.4, 2.6 |
| *IMC:SG2 Detect Events* | | |
| IMC:SG2.SP1 Detect and Report Events | 34R1 | 4.2 |
| | 53R4 | AR-4, AU-13, IA-10, IR-4, IR-5, IR-6, PE-6, RA-6 |
| | 61R2 | 3.2.4, 3.6 |
| IMC:SG2.SP2 Log and Track Events | 53R4 | IR-4, IR-5, IR-7 |
| | 61R2 | 3.2.5, 3.6 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence | 53R4 | IR-4, IR-5 |
| | 61R2 | 3.3.2, 3.4.3, 3.6 |
| IMC:SG2.SP4 Analyze and Triage Events | 53R4 | IR-4 |
| | 61R2 | 3.2.4, 3.2.6, 3.6 |
| *IMC:SG3 Declare Incidents* | | |
| IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria | 30R1 | App. E |
| | 34R1 | 4.2.1 |
| | 53R4 | IR-4 |
| IMC:SG3.SP2 Analyze Incidents | 34R1 | 4.2.3 |
| | 53R4 | IR-4 |
| | 61R2 | 3.3.3, 3.6 |
| *IMC:SG4 Respond to and Recover from Incidents* | | |
| IMC:SG4.SP1 Escalate Incidents | 53R4 | IR-4, IR-9 |
| | 61R2 | 3.2.6, 3.2.7, 3.6, 4.3.1, 4.4 |
| IMC:SG4.SP2 Develop Incident Response | 53R4 | IR-4, IR-9, SE-2 |
| | 61R2 | 3.3.1, 3.3.4, 3.6, 4, 4.1, 4.2, 4.4 |
| IMC:SG4.SP3 Communicate Incidents | 34R1 | 4.2.2 |
| | 53R4 | IR-4, IR-9 |
| | 61R2 | 2.3.4, 2.4.4, 2.6, 3.2.7, 3.6, 4, 4.1, 4.2, 4.3.2, 4.4 |
| IMC:SG4.SP4 Close Incidents | 53R4 | IR-4 |
| *IMC:SG5 Establish Incident Learning* | | |
| IMC:SG5.SP1 Perform Post-Incident Review | 53R4 | IR-4 |
| | 61R2 | 3.4.1, 3.6 |
| IMC:SG5.SP2 Integrate with the Problem Management Process | 53R4 | IR-4 |
| | 61R2 | 3.4.2 |
| | 137 | 3.4, 3.4.1, 3.4.2 |
| IMC:SG5.SP3 Translate Experience to Strategy | 53R4 | IR-4 |
| | 61R2 | 3.4.1, 3.4.2 |
| KIM – Knowledge and Information Management | | |
| *KIM:SG1 Establish and Prioritize Information Assets* | | |
| KIM:SG1.SP1 Prioritize Information Assets | 53R4 | SC-38 |
| KIM:SG1.SP2 Categorize Information Assets | 37R1 | 2.1 |
| | 53R4 | AC-22 |
| | 60V1R1 | 3.1.1, 4 |
| *KIM:SG2 Protect Information Assets* | | |
| KIM:SG2.SP1 Assign Resilience Requirements to Information Assets | 34R1 | 3.4.1, 3.4.2, |
| | 53R4 | AC-16, AC-21, DM-1, DM-3, IP-1, MP-2, SC-2 |
| | 53AR1 | 3.1 |
| | 60V1R1 | 3.1.2, 4 |
| KIM:SG2.SP2 Establish and Implement Controls | 34R1 | 3.4.1, 3.4.2 |
| | 53R4 | AC-16, AC-21, AC-23, AC-24, CP-12, DM-3, IA-9, MP-1, MP-2, MP-7, PE-5, SA-18, SC-2, SI-16 |
| | 53AR1 | 3.1 |
| | 137 | 3.3 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| *KIM:SG3 Manage Information Asset Risk* | | |
| KIM:SG3.SP1 Identify and Assess Information Asset Risk | 30R1 | 3.1, 3.2 |
| | 53R4 | PM-7 |
| KIM:SG3.SP2 Mitigate Information Asset Risk | 30R1 | 3.2 |
| | 53R4 | CP-11, CP-13, DM-1, DM-3, IA-10, PM-4, SA-20, SC-36, SC-37, SC-38, SC-39, SI-14 |
| | 137 | 3.5 |
| *KIM:SG4 Manage Information Asset Confidentiality and Privacy* | | |
| KIM:SG4.SP1 Encrypt High-Value Information | 53R4 | SC-8, SC-11, SC-12, SC-13, SC-17 |
| KIM:SG4.SP2 Control Access to Information Assets | 53R4 | AC-23, AC-25, AR-8, AU-13, IA-1, MP-3, MP-4, MP-5, SI-11 |
| KIM:SG4.SP3 Control Information Asset Disposition | 53R4 | AR-8, DM-2 MP-3, MP-4, MP-5, MP-6, MP-8 |
| *KIM:SG5 Manage Information Asset Integrity* | | |
| KIM:SG5.SP1 Control Modification of Information Assets | 53R4 | IP-3, SI-7 |
| KIM:SG5.SP2 Manage Information Asset Configuration | 53R4 | DI-1, SI-7 |
| KIM:SG5.SP3 Verify Validity of Information | 53R4 | DI-1, DI-2, SC-8, SC-20, SC-21, SI-7, SI-15 |
| *KIM:SG6 Manage Information Asset Availability* | | |
| KIM:SG6.SP1 Perform Information Duplication and Retention | 53R4 | CP-9, SI-12 |
| KIM:SG6.SP2 Manage Organizational Knowledge | | |
| MA – Measurement and Analysis | | |
| *MA:SG1 Align Measurement and Analysis Activities* | | |
| MA:SG1.SP1 Establish Measurement Objectives | 53R4 | PM-6 |
| | 53AR1 | 3.1, 3.2.1, 3.2.2, App. F |
| | 55R1 | 5.2, 5.5, 5.7, 6.1 |
| MA:SG1.SP2 Specify Measures | 53R4 | SA-15 |
| | 53AR1 | 3.2.2, App. F |
| | 55R1 | 5.5 |
| MA:SG1.SP3 Specify Data Collection and Storage Procedures | 55R1 | 3.4.3, 3.4.4, 5.5 |
| MA:SG1.SP4 Specify Analysis Procedures | 53AR1 | 3.2.2, App. D, App. F |
| | 55R1 | 5.7, 6.2 |
| *MA:SG2 Provide Measurement Results* | | |
| MA:SG2.SP1 Collect Measurement Data | 53AR1 | 3.3 |
| | 55R1 | 6.2 |
| MA:SG2.SP2 Analyze Measurement Data | 55R1 | 6.2 |
| MA:SG2.SP3 Store Data and Results | 55R1 | 3.4.3, 6.2 |
| MA:SG2.SP4 Communicate Results | 53R4 | SA-15 |
| | 53AR1 | App. G |
| | 55R1 | 6.2 |
| MON – Monitoring | | |
| *MON:SG1 Establish and Maintain a Monitoring Program* | | |
| MON:SG1.SP1 Establish a Monitoring Program | 53R4 | CA-7, PM-6, PM-14 |
| MON:SG1.SP2 Identify Stakeholders | 55R1 | 5.1 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| MON:SG1.SP3 Establish Monitoring Requirements | 53R4 | CA-7, PM-6, SI-4 |
| | 55R1 | 5.2 |
| | 70R2 | 3 |
| MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements | | |
| *MON:SG2 Perform Monitoring* | | |
| MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure | 53R4 | RA-5 |
| MON:SG2.SP2 Establish Collection Standards and Guidelines | 39 | 3.4 |
| | 53R4 | RA-5 |
| | 55R1 | 6.1 |
| MON:SG2.SP3 Collect and Record Information | 39 | 3.4 |
| | 53R4 | AR-6, CM-11, RA-5, SE-1, SI-4 |
| | 55R1 | 6.2 |
| | 137 | 3.4.2 |
| MON:SG2.SP4 Distribute Information | 39 | 3.4 |
| | 53R4 | AR-6, RA-5, SE-1, SI-4 |
| | 137 | 3.3, 3.4, 3.4.2, 3.4.3 |
| OPD – Organizational Process Definition | | |
| *OPD:SG1 Establish Organizational Process Assets* | | |
| OPD:SG1.SP1 Establish Standard Processes | 53R4 | AR-2, IP-4, PM-11, PM-14 |
| | 53AR1 | 3.2, App. D, App. E |
| OPD:SG1.SP2 Establish Tailoring Criteria and Guidelines | 53AR1 | 3.2, 3.2.3, 3.2.4 |
| OPD:SG1.SP3 Establish the Organization's Measurement Repository | 53AR1 | 3.2 |
| OPD:SG1.SP4 Establish the Organization's Process Asset Library | | |
| OPD:SG1.SP5 Establish Work Environment Standards | | |
| OPD:SG1.SP6 Establish Rules and Guidelines for Integrated Teams | | |
| OPF – Organizational Process Focus | | |
| *OPF:SG1 Determine Process Improvement Opportunities* | | |
| OPF:SG1.SP1 Establish Organizational Process Needs | | |
| OPF:SG1.SP2 Appraise the Organization's Processes | | |
| OPF:SG1.SP3 Identify the Organization's Process Improvements | 53AR1 | 3.2.5 |
| *OPF:SG2 Plan and Implement Process Actions* | | |
| OPF:SG2.SP1 Establish Process Action Plans | 53AR1 | 3.2.5 |
| OPF:SG2.SP2 Implement Process Action Plans | 53AR1 | 3.2.5 |
| *OPF:SG3 Deploy Organizational Process Assets and Incorporate Experiences* | | |
| OPF:SG3.SP1 Deploy Organizational Process Assets | | |
| OPF:SG3.SP2 Deploy Standard Processes | | |
| OPF:SG3.SP3 Monitor the Implementation | | |
| OPF:SG3.SP4 Incorporate Experiences into Organizational Process Assets | | |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| OTA – Organizational Training and Awareness | | |
| *OTA:SG1 Establish Awareness Program* | | |
| OTA:SG1.SP1 Establish Awareness Needs | 53R4 | AT-1 |
| OTA:SG1.SP2 Establish Awareness Plan | 53R4 | AR-5, AT-1, IP-1, PM-16 |
| OTA:SG1.SP3 Establish Awareness Delivery Capability | 53R4 | AT-1 |
| *OTA:SG2 Conduct Awareness Activities* | | |
| OTA:SG2.SP1 Perform Awareness Activities | 53R4 | AT-2, PM-15, PM-16 |
| OTA:SG2.SP2 Establish Awareness Records | 53R4 | AT-4 |
| OTA:SG2.SP3 Assess Awareness Program Effectiveness | | |
| *OTA:SG3 Establish Training Capability* | | |
| OTA:SG3.SP1 Establish Training Needs | 34R1 | 3.5 |
| | 53R4 | AT-1, SA-16 |
| OTA:SG3.SP2 Establish Training Plan | 34R1 | 3.5.1 |
| | 53R4 | AT-1, PM-13, UL-2 |
| OTA:SG3.SP3 Establish Training Capability | 53R4 | AT-1 |
| *OTA:SG4 Conduct Training* | | |
| OTA:SG4.SP1 Deliver Training | 53R4 | AR-5, AT-3, PM-14 |
| OTA:SG4.SP2 Establish Training Records | 53R4 | AT-4 |
| OTA:SG4.SP3 Assess Training Effectiveness | | |
| PM – People Management | | |
| *PM:SG1 Establish Vital Staff* | | |
| PM:SG1.SP1 Identify Vital Staff | | |
| *PM:SG2 Manage Risks Associated with Staff Availability* | | |
| PM:SG2.SP1 Identify and Assess Staff Risk | 53R4 | PM-7 |
| PM:SG2.SP2 Mitigate Staff Risk | 53R4 | PM-4, PM-7 |
| *PM:SG3 Manage the Availability of Staff* | | |
| PM:SG3.SP1 Establish Redundancy for Vital Staff | | |
| PM:SG3.SP2 Perform Succession Planning | 53R4 | PM-11 |
| PM:SG3.SP3 Prepare for Redeployment | | |
| PM:SG3.SP4 Plan to Support Staff During Disruptive Events | 53R4 | PM-11 |
| PM:SG3.SP5 Plan for Return-to-Work Considerations | 53R4 | PM-11 |
| RISK – Risk Management | | |
| *RISK:SG1 Prepare for Risk Management* | | |
| RISK:SG1.SP1 Determine Risk Sources and Categories | 30R1 | 3.1, 3.2, App. D, App. E |
| | 37R1 | 2.1 |
| | 39 | 3.2 |
| | 53R4 | RA-2 |
| | 61R2 | 3.1.2 |
| RISK:SG1.SP2 Establish an Operational Risk Management Strategy | 30R1 | 2, 3.1, 3.2 |
| | 37R1 | 2.1 |
| | 39 | 2.1, 2.2, 2.6, |
| | 53R4 | PM-9 |
| | 53AR1 | 3.1 |
| | 137 | 2.1, 2.1.1, 3.1, 3.1.1, 3.1.2, 3.1.3, 3.2, 3.2.3 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| *RISK:SG2 Establish Risk Parameters and Focus* | | |
| RISK:SG2.SP1 Define Risk Parameters | 30R1 | 3.1, 3.2 |
| | 39 | 2.2 |
| | 53R4 | CA-6, PM-9, RA-3 |
| | 53AR1 | 3.1 |
| | 137 | 2.1.1, 2.1.2 |
| RISK:SG2.SP2 Establish Risk Measurement Criteria | 30R1 | 3.1 |
| | 39 | 3.2 |
| | 53R4 | PM-9, RA-3, |
| | 53AR1 | 3.1 |
| | 55R1 | 5.5 |
| | 137 | 2.1.1, 3.2.1 |
| *RISK:SG3 Identify Risk* | | |
| RISK:SG3.SP1 Identify Asset-Level Risks | 30R1 | 3.2 |
| | 39 | 3.2 |
| | 53R4 | CA-2, PM-9, RA-3, SA-20 |
| | 60V1R1 | 4.2, 4.3, 4.4, 4.5 |
| RISK:SG3.SP2 Identify Service-Level Risks | 30R1 | 3.2 |
| | 39 | 3.2 |
| | 53R4 | PM-9, RA-3 |
| *RISK:SG4 Analyze Risk* | | |
| RISK:SG4.SP1 Evaluate Risk | 30R1 | 3.2, App. G, App. H, App. I |
| | 53R4 | PM-9, RA-3, SC-38 |
| | 137 | 3.1.3, 3.4.1 |
| RISK:SG4.SP2 Categorize and Prioritize Risk | 30R1 | 3.2, App. D, App. J |
| | 37R1 | 2.1 |
| | 53R4 | PM-9, RA-3 |
| RISK:SG4.SP3 Assign Risk Disposition | 53R4 | PM-9, RA-3 |
| | 137 | 3.1.3, 3.4.1, 3.5 |
| *RISK:SG5 Mitigate and Control Risk* | | |
| RISK:SG5.SP1 Develop Risk Mitigation Plans | 39 | 2.2 |
| | 53R4 | AR-2, CA-5, PM-4, PM-9, RA-3 |
| | 137 | 3.4.1 |
| RISK:SG5.SP2 Implement Risk Strategies | 30R1 | 3.3, 3.4, App. K |
| | 39 | 2.2 |
| | 53R4 | AR-2, PM-9, RA-3 |
| | 137 | 2.1.3, 3.1.3, 3.3, 3.5 |
| *RISK:SG6 Use Risk Information to Manage Resilience* | | |
| RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services | 53R4 | PM-9 |
| | 137 | 2.1.3, 2.2, 3.1.3, 3.6 |
| RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services | 53R4 | PM-9, PM-14 |
| | 137 | 3.6 |
| RRD – Resilience Requirements Development | | |
| *RRD:SG1 Identify Enterprise Requirements* | | |
| RRD:SG1.SP1 Establish Enterprise Resilience Requirements | 53R4 | AR-3, PM-7 |
| | 53AR1 | 2.3 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| *RRD:SG2 Develop Service Requirements* | | |
| RRD:SG2.SP1 Establish Asset Resilience Requirements | 18R1 | 1.8, 2 |
| | 53R4 | SA-2, SA-13 |
| | 53AR1 | 2.3, 3.1, 3.2.1 |
| | 60V1R1 | 4.6 |
| | 70R2 | 3 |
| RRD:SG2.SP2 Assign Enterprise Resilience Requirements to Services | 18R1 | 2.5.1, 2.5.3 |
| | 53R4 | PM-7 |
| *RRD:SG3 Analyze and Validate Requirements* | | |
| RRD:SG3.SP1 Establish a Definition of Required Functionality | 18R1 | 3.9 |
| RRD:SG3.SP2 Analyze Resilience Requirements | 53R4 | SA-13 |
| | 53AR1 | 3.1 |
| RRD:SG3.SP3 Validate Resilience Requirements | 53R4 | SA-13 |
| | 53AR1 | 3.1 |
| | 70R2 | 4 |
| RRM – Resilience Requirements Management | | |
| *RRM:SG1 Manage Requirements* | | |
| RRM:SG1.SP1 Obtain an Understanding of Resilience Requirements | 18R1 | 2.5 |
| | 53R4 | PM-7 |
| | 53AR1 | 3.1 |
| | 70R2 | 4 |
| RRM:SG1.SP2 Obtain Commitment to Resilience Requirements | 18R1 | 3 |
| | 53R4 | SA-2 |
| RRM:SG1.SP3 Manage Resilience Requirements Changes | 18R1 | 3 |
| | 60V1R1 | 4.6 |
| RRM:SG1.SP4 Maintain Traceability of Resilience Requirements | 18R1 | 3 |
| RRM:SG1.SP5 Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements | 53R4 | PM-7 |
| | 53AR1 | 3.1 |
| RTSE – Resilient Technical Solution Management | | |
| *RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development* | | |
| RTSE:SG1.SP1 Identify General Guidelines | 37R1 | 2.2 |
| | 53R4 | SA-4, SA-15, SI-17 |
| | 70R2 | 3 |
| RTSE:SG1.SP2 Identify Requirements Guidelines | 53R4 | SA-4, SA-13 |
| | 70R2 | 3 |
| RTSE:SG1.SP3 Identify Architecture and Design Guidelines | 53R4 | AR-7, PL-8, SA-4, SA-17 |
| | 70R2 | 3 |
| RTSE:SG1.SP4 Identify Implementation Guidelines | 53R4 | SA-4, SA-11 |
| RTSE:SG1.SP5 Identify Assembly and Integration Guidelines | 53R4 | SA-4, SA-11 |
| *RTSE:SG2 Develop Resilient Technical Solution Development Plans* | | |
| RTSE:SG2.SP1 Select and Tailor Guidelines | 18R1 | 2.5 |
| | 53R4 | SA-12, SA-14 |
| | 70R2 | 4 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process | 37R1 | 2.2 |
| | 53R4 | PM-7, SA-3, SA-12, SA-14 |
| *RTSE:SG3 Execute the Plan* | | |
| RTSE:SG3.SP1 Monitor Execution of the Development Plan | 53R4 | SA-12, SA-14 |
| RTSE:SG3.SP2 Release Resilient Technical Solutions into Production | 53R4 | SA-12, SA-14 |
| SC – Service Continuity | | |
| *SC:SG1 Prepare for Service Continuity* | | |
| SC:SG1.SP1 Plan for Service Continuity | 34R1 | 3.1, 3.4 |
| | 53R4 | CP-1, CP-13, PM-11 |
| SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity | 34R1 | 3.1, 4 |
| *SC:SG2 Identify and Prioritize High-Value Services* | | |
| SC:SG2.SP1 Identify the Organization's High-Value Services | 34R1 | 3.2 |
| | 53R4 | CP-2 |
| SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies | 34R1 | 3.2 |
| | 53R4 | SC-8 |
| SC:SG2.SP3 Identify Vital Organizational Records and Databases | 34R1 | 3.2 |
| | 53R4 | SC-8 |
| *SC:SG3 Develop Service Continuity Plans* | | |
| SC:SG3.SP1 Identify Plans to Be Developed | 53R4 | CP-10, PM-11 |
| SC:SG3.SP2 Develop and Document Service Continuity Plans | 34R1 | 3.4 |
| | 53R4 | CP-2 |
| SC:SG3.SP3 Assign Staff to Service Continuity Plans | 34R1 | 3.4.6 |
| | 53R4 | CP-2 |
| SC:SG3.SP4 Store and Secure Service Continuity Plans | | |
| SC:SG3.SP5 Develop Service Continuity Plan Training | 34R1 | 3.5.2 |
| | 53R4 | CP-3, IR-2 |
| *SC:SG4 Validate Service Continuity Plans* | | |
| SC:SG4.SP1 Validate Plans to Requirements and Standards | | |
| SC:SG4.SP2 Identify and Resolve Plan Conflicts | | |
| *SC:SG5 Exercise Service Continuity Plans* | | |
| SC:SG5.SP1 Develop Testing Program and Standards | | |
| SC:SG5.SP2 Develop and Document Test Plans | 53R4 | CP-4 |
| SC:SG5.SP3 Exercise Plans | 34R1 | 3.5.3 |
| | 53R4 | CP-3, CP-4 |
| SC:SG5.SP4 Evaluate Plan Test Results | 53R4 | CP-4 |
| *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 | 34R1 | 3.6 |
| | 53R4 | CP-2 |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| TM – Technology Management | | |
| *TM:SG1 Establish and Prioritize Technology Assets* | | |
| TM:SG1.SP1 Prioritize Technology Assets | 34R1 | 3.2.3 |
| | 53R4 | PL-2, PM-5, SA-14, SA-20 |
| TM:SG1.SP2 Establish Resilience-Focused Technology Assets | 53R4 | PM-5, SA-14 |
| *TM:SG2 Protect Technology Assets* | | |
| TM:SG2.SP1 Assign Resilience Requirements to Technology Assets | 18R1 | 3.2 |
| | 53R4 | AC-14, CM-6, CM-7, PL-2, SA-13, SC-2 |
| | 53AR1 | 3.1 |
| | 60V1R1 | 3.1, 4 |
| | 70R2 | 3 |
| TM:SG2.SP2 Establish and Implement Controls | 18R1 | 2.5, 3.13, 3.14 |
| | 34R1 | 3.3 |
| | 53R4 | AC-14, AU-3, AU-7, AU-8, AU-9, AU-10, AU-12, AU-14, CA-9, CM-7, CP-12, MP-7, PE-5, PL-2, PM-7, SC-39, SC-40, SC-41, SC-42, SC-43, SI-6 |
| | 53AR1 | 3.1 |
| | 137 | 3.3 |
| *TM:SG3 Manage Technology Asset Risk* | | |
| TM:SG3.SP1 Identify and Assess Technology Asset Risk | 30R1 | 3.1, 3.2 |
| | 53R4 | CM-4, PM-7, PM-10 |
| TM:SG3.SP2 Mitigate Technology Risk | 30R1 | 3.2 |
| | 34R1 | 3.3 |
| | 53R4 | PM-4, PM-7, PM-10, SA-20 |
| | 137 | 3.5 |
| *TM:SG4 Manage Technology Asset Integrity* | | |
| TM:SG4.SP1 Control Access to Technology Assets | 18R1 | 2.5, 3.13, 3.14 |
| | 53R4 | AC-3, AC-4, AC-7, AC-8, AC-9, AC-11, AC-17, AC-18, AC-19, AC-25, CM-5, IA-3, IA-5, IA-6, IA-7, IA-8, MA-1, MA-3, MA-4, MA-5, SA-18, SC-43, SI-7 |
| TM:SG4.SP2 Perform Configuration Management | 18R1 | 3.16 |
| | 53R4 | AC-19, CM-1, CM-2, CM-3, CM-6, CM-9, SA-5, SA-10, SI-2, SI-7 |
| TM:SG4.SP3 Perform Change Control and Management | 18R1 | 3.16 |
| | 53R4 | CM-3, CM-4, SA-10, SI-7 |
| TM:SG4.SP4 Perform Release Management | 53R4 | IA-2, PM-10, SI-7 |
| *TM:SG5 Manage Technology Asset Availability* | | |
| TM:SG5.SP1 Perform Planning to Sustain Technology Assets | 34R1 | 3.4.4 |
| | 53R4 | AU-15, PE-11, PM-11, SA-22, SI-13 |
| TM:SG5.SP2 Manage Technology Asset Maintenance | 53R4 | AU-5, MA-2, MA-4, MA-6 |
| TM:SG5.SP3 Manage Technology Capacity | 53R4 | AU-4 |
| TM:SG5.SP4 Manage Technology Interoperability | 18R1 | 3.11 |
| VAR – Vulnerability Analysis and Resolution | | |
| *VAR:SG1 Prepare for Vulnerability Analysis and Resolution* | | |
| VAR:SG1.SP1 Establish Scope | 53AR1 | 2.2, 2.3, 3.2, App. D, App. E |
| | 70R2 | 3 |
| VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy | 30R1 | 3.2 |
| | 53AR1 | 2.2, 2.3, 2.4, 3.2, App. D, App. E, App. F |

| CERT-RMM V1.1 Process Areas, Goals, and Specific Practices | NIST Special Publications | |
|---|---|---|
| | SP No. 800- | Section Numbers Related to the NIST Publication (Control Numbers for 800-53 Rev. 4) |
| *VAR:SG2 Identify and Analyze Vulnerabilities* | | |
| VAR:SG2.SP1 Identify Sources of Vulnerability Information | 30R1 | 3.1, 3.2, App. D, App. E, App. F |
| | 53R4 | CA-8, RA-5, RA-6 |
| | 61R2 | 3.1.2 |
| VAR:SG2.SP2 Discover Vulnerabilities | 30R1 | 3.2 |
| | 34R1 | 3.3 |
| | 53R4 | CA-8, RA-5, SA-10, SA-11, SI-2, SI-3 |
| VAR:SG2.SP3 Analyze Vulnerabilities | 30R1 | 3.2 |
| | 53R4 | RA-5, SA-10, SA-11, SC-38, SI-2, SI-3 |
| *VAR:SG3 Manage Exposure to Vulnerabilities* | | |
| VAR:SG3.SP1 Manage Exposure to Vulnerabilities | 34R1 | 3.3 |
| | 53R4 | RA-5, SA-10, SA-11, SI-2, SI-3 |
| | 61R2 | 3.1.2, 3.6 |
| *VAR:SG4 Identify Root Causes* | | |
| VAR:SG4.SP1 Perform Root-Cause Analysis | 53R4 | RA-5, SA-11, SI-2 |

# References

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


**[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 800-55 Revision 1, Performance Measurement Guide for Information Security.* NIST, 2008. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

**[NIST 2008b]**
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 2008c]**
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 2010a]**
National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-34 Revision 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 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems.* NIST, 2010. http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

**[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

**[NIST 2011c]**
National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* NIST, 2011. http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

**[NIST 2012a]**
National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.* NIST, 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

**[NIST 2012b]**
National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide.* NIST, 2012. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

**[NIST 2013]**
National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.* NIST, 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

**[Partridge 2011a]**
Partridge, Kevin; & Young, Lisa. *CERT® Resilience Management Model (RMM) v1.1: Code of Practice Crosswalk Commercial Version 1.1* (CMU/SEI-2011-TN-012 ). Software Engineering Institute, Carnegie Mellon University, 2011. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9849

**[Partridge 2011b]**
Partridge, Kevin; & Young, Lisa. *CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1* (CMU/SEI-2011-TN-028). Software Engineering Institute, Carnegie Mellon University, 2011. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9881

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. AGENCY USE ONLY | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| (Leave Blank) | June 2014 | Final |

| 4. TITLE AND SUBTITLE | 5. FUNDING NUMBERS |
|---|---|
| CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 2 | FA8721-05-C-0003 |

6. AUTHOR(S)

Kevin G. Partridge, Mary E. Popeck, and Lisa R. Young

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| Software Engineering Institute<br>Carnegie Mellon University<br>Pittsburgh, PA 15213 | CMU/SEI-2014-TN-004 |

| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER |
|---|---|
| AFLCMC/PZE/Hanscom<br>Enterprise Acquisition Division<br>20 Schilling Circle<br>Building 1305<br>Hanscom AFB, MA 01731-2116 | |

11. SUPPLEMENTARY NOTES

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

13. abstract (maximum 200 words)

The CERT® Resilience Management Model (CERT®-RMM) 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) and an update to the *CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1* (CMU/SEI-2011-TN-028).

| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| NIST, Special Publication, Security, Model, RMM, Resilience, Risk | 29 |

16. PRICE CODE

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