Software Engineering Institute

CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication 800-66 Crosswalk

Lisa R. Young, Software Engineering Institute
Ma-Nyahn Kromah, SunGard Availability Services

October 2013

TECHNICAL NOTE
CMU/SEI-2013-TN-027

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by SunGard Availability Services 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 SunGard Availability Services or 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-0000666

Table of Contents

Acknowledgments

Many individuals have contributed to this report by giving generously of their time and expertise. Their contributions are expressed in the form of ideas, concepts, reviews, edits, and recommendations. The authors extend thanks and appreciation to Chris Burgher of SunGard Availability Services for his support, knowledge, and efforts in developing this document; William Gouveia of SunGard Availability Services; Pete Sullivan of InfoSecure Solutions, LLC; Summer Fowler, Technical Manager of the CERT® Cyber Resilience Team; and Rich Caralli, Technical Director of the CERT Cyber Enterprise and Workforce Management Directorate. We also very much appreciate the fine technical editing and visual enhancement to the document that Paul Ruggiero of the SEI provided.

Abstract

Organizations can use the CERT® Resilience Management Model (CERT®-RMM) V1.1, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute, to determine how their current practices can support their level of process maturity in areas of operational resilience (business continuity, disaster recovery, management and security planning, and IT operations and service delivery). This technical note is a follow-on to the *CERT-RMM Code of Practice Crosswalk, Commercial Version 1.1* (CMU/SEI-2011-TN-012) and connects CERT-RMM process areas to *NIST Special Publication 800-66 Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*.

1 Introduction

Organizations can use the CERT® Resilience Management Model (CERT®-RMM) V1.1, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute, to determine how their current practices can support their level of process maturity in areas of operational resilience (business continuity, disaster recovery, management and security planning, and IT operations and service delivery). This technical note is a follow-on to the *CERT-RMM Code of Practice Crosswalk, Commercial Version 1.1* (CMU/SEI-2011-TN-012) [Partridge 2011a] and connects CERT-RMM process areas to *NIST Special Publication 800-66 Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* [Scholl 2008].

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

The key activities, and their descriptions, of the CERT-RMM process areas align with the guidance within NIST SP 800-66. The crosswalk in this technical note does not reflect any discontinuities at this level between the two. It connects NIST SP 800-66 key activities and CERT-RMM goals, practices, and general goals according to their shared subject matter and focus.

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:

- 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 includes references to 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 is organized by several key components. The process area is the major structural element in the model. Each process area has a series of descriptive components. CERT-RMM has two types of practices: specific practices and subpractices. The subpractices are the level at which CERT-RMM connects with specific guidance in codes of practice or standards. To make use of and gain key benefits from the crosswalk presented in this document, it is important to understand the distinctions among these types of practices and subpractices in CERT-RMM and their connection to the HIPAA Security Rule.

Process Area

CERT-RMM has four categories—enterprise management, engineering, operations, and process management—which together comprise 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.

Process Area: 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 Risk Management process area is "RISK:SG1 Prepare for Risk Management."

Process Area: Specific Practices

Each process area goal has its own specific practices. Specific practices establish a process area's base practices, reflect its body of knowledge, and describe what must be done to accomplish a process area goal. An example of a specific practice from the Risk Management process area is "RISK:SG1.SP1 Determine Risk Sources and Categories," which supports the goal "RISK:SG1 Prepare for Risk Management."

Process Area: 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 HIPAA Security Rule found in NIST SP 800-66.

Generic Goals

Generic goals are relevant to all process areas but are defined within and customized to individual process areas. Their degree of achievement indicates an organization's integration of a process's level into its fundamental values (policies, standards, code of conduct, strategic plans, values, vision, etc.). 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.

This crosswalk is not intended to map the NIST SP 800-66 HIPAA Security Privacy Rule across all generic goals or assert that a special publication helps an organization achieve any particular capability or maturity rating.

2 NIST Special Publication 800-66

Special Publication 800-66 (SP 800-66) Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule is a publication from the National Institute of Standards and Technology for United States federal government agencies that may be subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA was enacted with two major goals: Title I of HIPAA protects health insurance coverage for workers and their families when they lose or change jobs, and Title II of HIPAA requires the establishment of national standards for electronic health care transactions and the security of patient data. Title II of HIPAA contains two important provisions for the protection of patient data, the Privacy Rule and the Security Rule.

NIST SP 800-66 focuses exclusively on the implementation of the HIPAA Security Rule. NIST SP 800-66 does not cover other elements of HIPAA (i.e., the HIPAA Privacy Rule). Additionally, NIST SP 800-66 does not cover the extensions to the HIPAA Security Rule by the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The HITECH Act is part of the American Recovery and Reinvestment Act of 2009.

This crosswalk between CERT-RMM and NIST SP 800-66 covers only the Administrative Safeguards, Physical Safeguards, and Technical Safeguards of the HIPAA Security Rule. It does not cover the organizational components or the Policies and Procedures and Documentation Requirements of the HIPAA Security Rule.

2.1 The HIPAA Security Rule

The HIPAA Security Rule protects all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is defined as Electronic Protected Health Information (e-PHI). The Security Rule covers only protected health information that is electronic in nature, not information that is transmitted orally or in written form.

The Security Rule requires maintenance of reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Organizations handling e-PHI must

- ensure the confidentiality, integrity, and availability of all e-PHI created, received, maintained or transmitted
- identify and protect against reasonably anticipated threats to the security or integrity of information
- protect against reasonably anticipated, impermissible uses or disclosures
- ensure compliance by the workforce

2.1.1 HIPAA Security Rule Safeguards

The HIPAA Security Rule defines safeguards in several areas:

- Administrative Safeguards—"Administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect

electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

- Physical Safeguards—"Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."
- Technical Safeguards—"The technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

NIST SP 800-66 describes the following Administrative, Physical, and Technical Safeguards:

Administrative Safeguards

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Technical Safeguards

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

3 NIST SP 800-66 to CERT-RMM Crosswalk

This crosswalk describes the mapping between CERT-RMM and NIST SP 800-66. All of the Administrative, Physical, and Technical Safeguards described in NIST SP 800-66 are mapped to specific practices within a CERT-RMM process area. This crosswalk aligns the tactical practices suggested in NIST SP 800-66 to the CERT-RMM process areas and specific practices that describe management of operational resilience at a process level.

This technical note shows the areas of connection between CERT-RMM process areas and the guidance in NIST SP 800-66. The CERT-RMM provides a reference model that allows organizations to make sense of their practices in a process context to improve processes and effectiveness. This crosswalk can help organizations align NIST SP 800-66 practices to CERT-RMM process improvement goals, with the overall goal of using CERT-RMM to manage compliance with the HIPAA Security Rule.

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.1. Security Management Process (C.E.R. § 164.308(a)(1)) **HIPAA Standard:** *Implement policies and procedures to prevent, detect, contain, and correct security violations.*	
1. Identify Relevant Information Systems • Identify all information systems that house e-PHI. • Include all hardware and software that are used to collect, store, process, or transmit e-PHI. • Analyze business functions and verify ownership and control of information system elements as necessary.	• ADM:SG1.SP1 Inventory Assets • ADM:SG1.SP3 Identify Asset Owner & Custodians • KIM:SG1.SP1 Prioritize Information Assets
2. Conduct Risk Assessment Implementation Specification (Required) • Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the covered entity.	• RISK:SG4.SP1 Evaluate Risk • RISK:SG4.SP2 Categorize and Prioritize Risk • RISK:GG2.GP4 Assign Responsibility
3. Implement a Risk Management Program Implementation Specification (Required) • Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	• RISK:SG5.SP2 Implement Risk Strategies • RISK:SG5.SP1 Develop Risk Mitigation Pans • RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services • RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services
4. Acquire IT Systems and Services • Although the HIPAA Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to adequately protect information. Considerations for their selection should include the following: ◦ Applicability of the IT solution to the intended environment; ◦ The sensitivity of the data; ◦ The organization's security policies, procedures, and standards; and ◦ Other requirements such as resources available for operation, maintenance, and training.	• TM:SG2.SP1 Assign Resilience Requirements to Technology Assets • TM:SG2.SP2 Establish and Implement Controls

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.1. Security Management Process (C.E.R. § 164.308(a)(1)) **HIPAA Standard:** *Implement policies and procedures to prevent, detect, contain, and correct security violations.*	

(continued)

5. Create and Deploy Policies and Procedures • Implement the decisions concerning the management, operational, and technical controls selected to mitigate identified risks. • Create policies that clearly establish roles and responsibilities and assign ultimate responsibility for the implementation of each control to particular individuals or offices. • Create procedures to be followed to accomplish particular security-related tasks.	• RISK:SG5.SP1 Develop Risk Mitigation Plan • GG2.GP1 Establish Process Governance • GG2.GP4 Assign Responsibility • GG2.GP7 Identify and Involve Relevant Stakeholders
6. Develop and Implement a Sanction Policy Implementation Specification (Required) • Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. • Develop policies and procedures for imposing appropriate sanctions (e.g., reprimand, termination) for noncompliance with the organization's security policies. • Implement sanction policy as cases arise.	• HRM:SG3.SP4 Establish Disciplinary Process
7. Develop and Deploy the Information System Activity Review Process Implementation Specification (Required) • Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	• TM:SG2.SP2 Establish and Implement Controls • IMC:SG2.SP2 Log and Track Events • EF:SG4.SP2 Perform Resilience Oversight
8. Develop Appropriate Standard Operating Procedures • Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports.	• MON:SG2.SP2 Establish Collection Standard and Guidelines • MON:SG1.SP3 Establish Monitoring Requirements • MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements
9. Implement the Information System Activity Review and Audit Process • Activate the necessary review process. • Begin auditing and logging activity.	• MON:SG1.SP3 Establish Monitoring Requirements • MON:SG2.SP2 Establish Collection Standard and Guidelines • COMP:SG4.SP1 Evaluate Compliance Activities

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.2. Assigned Security Responsibility (C.E.R. § 164.308(a)(2)) **HIPAA Standard:** *Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.*	
1. Select a Security Official To Be Assigned Responsibility for HIPAA Security • Identify the individual who has final responsibility for security. • Select an individual who is able to assess effective security and to serve as the point of contact for security policy, implementation, and monitoring.	• EF:SG4.SP1 Establish Resilience as a Governance Focus Area • EF:GG2.GP2 Plan the Process • EF:GG2.G4 Assign Responsibility • IMC:GG2.GP2 Plan the Process • IMC:GG2.GP4 Assign Responsibility
2. Assign and Document the Individual's Responsibility • Document the assignment to one individual's responsibilities in a job description. • Communicate this assigned role to the entire organization.	• EF & IMC:GG2.GP2 Plan the Process • EF & IMC:GG2.G4 Assign Responsibility • HRM:SG2.SP2 Establish Terms and Conditions of Employment • PM:SG1.SP1 Identify Vital Staff • GG2 & GG4

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.3. Workforce Security (C.E.R. § 164.308(a)(3)) **HIPAA Standard:** *Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.*	
1. Implement Procedures for Authorization and/or Supervision Implementation Specification (Addressable) • Implement procedures for the authorization and/or supervision of workforce members who work with e-PHI or in locations where it might be accessed.	• AM:SG1 Manage and Control Access (SP1-SP4) • ID:SG2.SP2 Periodically Review and Maintain Identities

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.3. Workforce Security (C.E.R. § 164.308(a)(3)) **HIPAA Standard:** *Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.*	

(continued)

2. Establish Clear Job Descriptions and Responsibilities • Define roles and responsibilities for all job functions. • Assign appropriate levels of security oversight, training, and access. • Identify in writing who has the business need—and who has been granted permission—to view, alter, retrieve, and store e-PHI, and at what times, under what circumstances, and for what purposes.	• HRM:SG2.SP2 Establish Terms and Conditions for Employment • ID:SG1.SP3 Assign Roles and Identities • AM:SG1.SP1 Enable Access • HRM:SG4.SP2 Manage Access to Assets
3. Establish Criteria and Procedures for Hiring and Assigning Tasks • Ensure that staff members have the necessary knowledge, skills, and abilities to fulfill particular roles, e.g., positions involving access to and use of sensitive information. • Ensure that these requirements are included as part of the personnel hiring process.	• HRM:SG2.SP2 Establish Terms and Conditions for Employment • HRM:SG3.SP1 Establish Resilience as a Job Responsibility • AM:SG1.SP3 Periodically Review and Maintain Access Privileges • AM:SG1.SP4 Correct Inconsistencies
4. Establish a Workforce Clearance Procedure Implementation Specification (Addressable) • Implement procedures to determine that the access of a workforce member to e-PHI is appropriate. • Implement appropriate screening of persons who will have access to e-PHI. • Implement a procedure for obtaining clearance from appropriate offices or individuals where access is provided or terminated.	• HRM:SG2.SP1 Verify Suitability of Candidate Staff • HRM:SG4.SP2 Manage Access to Assets • HRM:SG4.SP3 Manage Involuntary Terminations • AM:SG1.SP1 Enable Access • AM:SG1.SP3 Periodically Review and Maintain Access Privileges • AM:SG1.SP4 Correct Inconsistencies

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.3. Workforce Security (C.E.R. § 164.308(a)(3)) **HIPAA Standard:** *Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.*	
(continued)	
5. Establish Termination Procedures Implementation Specification (Addressable) • Implement procedures for terminating access to e-PHI when the employment of a workforce member ends or as required by determinations made as specified in §164.308(a)(3)(ii)(B). • Develop a standard set of procedures that should be followed to recover access control devices (Identification [ID] badges, keys, access cards, etc.) when employment ends. • Deactivate computer access accounts (e.g., disable user IDs and passwords). See the Access Controls Standard.	• HRM:SG4.SP1 Manage Impact of Position Changes • HRM:SG4.SP2 Manage Access to Assets • HRM:SG4.SP3 Manage Involuntary Termination

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.4. Information Access Management (C.E.R. § 164.308(a)(4)) **HIPAA Standard:** *Implement policies and procedures to prevent, detect, contain, and correct security violations.*	
1. Isolate Healthcare Clearinghouse Functions Implementation Specification (Required) • If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the e-PHI of the clearinghouse from unauthorized access by the larger organization. • Determine if a component of the covered entity constitutes a healthcare clearinghouse under the HIPAA Security Rule. • If no clearinghouse functions exist, document this finding. If a clearinghouse exists within the organization, implement procedures for access consistent with the HIPAA Privacy Rule.	• KIM:SG4.SP2 Control Access to Information Assets • EXD:SG2.SP2 Mitigate Risk Due to External Dependencies • ADM:SG1.SP3 Establish Ownership and Custodianship • ADM:SG2.SP2 Analyze Asset-Service Dependencies

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.4. Information Access Management (C.E.R. § 164.308(a)(4)) **HIPAA Standard:** *Implement policies and procedures to prevent, detect, contain, and correct security violations.*	

(continued)

2. Implement Policies and Procedures for Authorizing Access Implementation Specification (Addressable) • Implement policies and procedures for granting access to e-PHI, for example, through access to a workstation, transaction, program, process, or other mechanism. • Decide how access will be granted to workforce members within the organization. • Select the basis for restricting access. • Select an access control method (e.g., identity-based, role-based, or other reasonable and appropriate means of access.) • Determine if direct access to e-PHI will ever be appropriate for individuals external to the organization (e.g., business partners or patients seeking access to their own e-PHI).	• AM:SG1 Manage and Control Access (SP1-SP4) • TM:SG4.SP1 Control Access to Technology Assets
3. Implement Policies and Procedures for Access Establishment and Modification Implementation Specification (Addressable) • Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. • Establish standards for granting access. • Provide formal authorization from the appropriate authority before granting access to sensitive information.	• KIM:SG4.SP2 Control Access to Information Assets • AM:SG1 Manage and Control Access (SP1-SP4) • AM:GG2.GP1 Establish Process Governance
4. Evaluate Existing Security Measures Related to Access Controls • Evaluate the security features of access controls already in place, or those of any planned for implementation, as appropriate. • Determine if these security features involve alignment with other existing management, operational, and technical controls, such as policy standards and personnel procedures, maintenance and review of audit trails, identification and authentication of users, and physical access controls.	• AM:SG1 Manage and Control Access (SP1-SP4) • AM:GG2.GP1 Establish Process Governance • KIM:SG4.SP2 Control Access to Information Assets • CTRL:SG4.SP1 Assess Controls

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.5. Security Awareness and Training (C.E.R. § 164.308(a)(5)) **HIPAA Standard:** *Implement a security awareness and training program for all members of its workforce (including management).*	
1. Conduct a Training Needs Assessment • Determine the training needs of the organization. • Interview and involve key personnel in assessing security training needs.	• OTA:SG1 Establish Awareness Program • OTA:SG3.SP2 Establish Training Needs • GG2.GP5 Train People
2. Develop and Approve a Training Strategy and a Plan • Address the specific HIPAA policies that require security awareness and training in the security awareness and training program. • Outline in the security awareness and training program the scope of the awareness and training program; the goals; the target audiences; the learning objectives; the deployment methods, evaluation, and measurement techniques; and the frequency of training.	• OTA:SG3 Establish Training Capability (SP1-SP3) • OTA:SG4 Conduct Training (SP1-SP3) • GG2.GP5 Train People • COMM:SG1.SP2 Identify Communications Requirements • COMM:SG2.SP1 Establish a Resilience Communications Plan • COMM:SG2.SP2 Establish a Resilience Communications Program • GG2.GP2 Plan the Process
3. Protection from Malicious Software; Log-in Monitoring; and Password Management Implementation Specifications (All Addressable) • As reasonable and appropriate, train employees regarding procedures for: ◦ Guarding against, detecting, and reporting malicious software; ◦ Monitoring log-in attempts and reporting discrepancies; and ◦ Creating changing, and safeguarding passwords. • Incorporate information concerning staff members' roles and responsibilities in implementing these implementation specifications into training and awareness efforts.	• OTA:SG2.SP3 Assess Awareness Program Effectiveness • OTA:SG3.SP3 Establish Training Capability • VAR:SG3.SP1 Manage Exposure to Vulnerabilities • VAR:GG2.GP2 Plan the Process • KIM:GG2.GP5 Train People

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.5. Security Awareness and Training (C.E.R. § 164.308(a)(5)) **HIPAA Standard:** *Implement a security awareness and training program for all members of its workforce (including management).*	

(continued)

4. Develop Appropriate Awareness and Training Content, Materials, and Methods • Select topics that may need to be included in the training materials. • Incorporate new information from email advisories, online IT security daily news Web sites, and periodicals, as is reasonable and appropriate. • Consider using a variety of media and avenues according to what is appropriate for the organization based on workforce size, location, level of education, etc.	• COMM:SG1.SP2 Identity Communication Requirements • COMM:SG2.SP1 Establish a Resilience Communication Plan • COMM:SG2.SP2 Establish a Resilience Communication Program • OTA:SG2 Conduct Awareness Activities (SP1-SP3) • OTA:SG3.SP3 Establish Training Capability • GG2.GP2 Plan the Process • GG2.GP5 Train People
5. Implement the Training • Schedule and conduct the training outlined in the strategy and plan. • Implement any reasonable technique to disseminate the security messages in an organization, including newsletters, screensavers, videotapes, email messages, teleconferencing sessions, staff meetings, and computer-based training.	• COMM:SG1.SP2 Identity Communication Requirements • COMM:SG2.SP1 Establish a Resilience Communication Plan • COMM:SG2.SP2 Establish a Resilience Communication Program • OTA:SG2.SP1 Deliver Resilience Training • GG2.GP2 Plan the Process • GG2.GP5 Train People

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.5. Security Awareness and Training (C.E.R. § 164.308(a)(5)) **HIPAA Standard:** *Implement a security awareness and training program for all members of its workforce (including management).*	
(continued)	
6. Implement Security Reminders Implementation Specification (Addressable) • Implement periodic security updates. • Provide periodic security updates to staff, business associates, and contractors.	• COMM:SG1.SP2 Identity Communication Requirements • COMM:SG2.SP1 Establish a Resilience Communication Plan • COMM:SG2.SP2 Establish a Resilience Communication Program • OTA:SG4.SP3 Assess Training Effectiveness • GG2.GP1 Establish Process Governance • GG2.GP2 Plan the Process • GG2.GP5 Train People
7. Monitor and Evaluate Training Plan • Keep the security awareness and training program current. • Conduct training whenever changes occur in the technology and practices as appropriate. • Monitor the training program implementation to ensure that all employees participate. • Implement corrective actions when problems arise.	• COMM:SG1.SP2 Identity Communication Requirements • COMM:SG2.SP1 Establish a Resilience Communication Plan • COMM:SG2.SP2 Establish a Resilience Communication Program • OTA:SG4.SP3 Assess Training Effectiveness • OTA:SG4.SP2 Establish Training Records • GG2.GP2 Plan the Process • GG2.GP5 Train People

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.6. Security Incident Procedures (C.E.R. § 164.308(a)(6)) **HIPAA Standard:** *Implement policies and procedures to address security incidents.*	
1. Determine Goals of Incident Response • Gain an understanding as to what constitutes a true security incident. Under the HIPAA Security Rule, a security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 CFR § 164.304) • Determine how the organization will respond to a security incident. • Establish a reporting mechanism and a process to coordinate responses to the security incident. • Provide direct technical assistance, advise vendors to address product-related problems, and provide liaisons to legal and criminal investigative groups as needed.	• IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria • IMC:SG4 Respond to and Recover from Incidents (SP1-SP2) • IMC:SG5.SP1 Perform Post-Incident Review
2. Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism • Determine if the size, scope, mission, and other aspects of the organization justify the reasonableness and appropriateness of maintaining a standing incident response team. • Identify appropriate individuals to be a part of a formal incident response team, if the organization has determined that implementing an incident response team is reasonable and appropriate.	• IMC:SG1.SP2 Assign Staff to the Incident Management Plan • IMC:SG4.SP2 Develop Incident Response • IMC:GG2.SP5 Train People • SC:SG3.SP3 Assign Staff to Service Continuity Plans
3. Develop and Implement Procedures to Respond to and Report Security Incidents Implementation Specification (Required) • Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. • Document incident response procedures that can provide a single point of reference to guide the day-to-day operations of the incident response team. • Review incident response procedures with staff with roles and responsibilities related to incident response, solicit suggestions for improvements, and make changes to reflect input if reasonable and appropriate. • Update the procedures as required based on changing organizational needs.	• IMC:SG1.SP1 Plan for Incident Management • IMC:SG2 Detect Event (SP1-SP4) • IMC:SG4.SP2 Develop Incident Response • IMC:SG5.SP3 Translate Experience to Strategy
4. Incorporate Post-Incident Analysis into Updates and Revisions • Measure effectiveness and update security incident response procedures to reflect lessons learned, and identify actions to take that will improve security controls after a security incident.	• IMC:SG5 Establish Incident Learning (SP1-SP3)

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.7. Contingency Plan (C.E.R. § 164.308(a)(7)) **HIPAA Standard:** *Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.*	
1. Develop Contingency Planning Policy • Define the organization's overall contingency objectives. • Establish the organizational framework, roles, and responsibilities for this area. • Address scope, resource requirements, training, testing, plan maintenance, and backup requirements.	• SC:SG1.SP1 Plan for Service Continuity • SC:SG1.SP2 Establish Standard and Guidelines for Service Continuity • SC:SG2 Identify and Prioritize High-Value Services (SP1-SP3)
2. Conduct an Applications and Data Criticality Analysis Implementation Specification (Addressable) • Assess the relative criticality of specific applications and data in support of other Contingency Plan components. • Identify the activities and material involving e-PHI that are critical to business operations. • Identify the critical services or operations, and the manual and automated processes that support them, involving e-PHI. • Determine the amount of time the organization can tolerate disruptions to these operations, material, or services (e.g., due to power outages). • Establish cost-effective strategies for recovering these critical services or processes.	• SC:SG2 Identify and Prioritize High-Value Services (SP1-SP3) • SC:SG4.SP1 Validate Plans to Requirements and Standards • FRM:SG2.SP1 Define Funding Needs
3. Identify Preventive Measures • Identify preventive measures for each defined scenario that could result in loss of a critical service operation involving the use of e-PHI. • Ensure that identified preventive measures are practical and feasible in terms of their applicability in a given environment.	• KIM:SG3 Manage Information Asset Risk (SP1-SP2) • RISK:SG3 Identify Risk • RISK:SG4 Analyze Risk • RISK:SG5 Mitigate and Control Risk

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.6. Security Incident Procedures (C.E.R. § 164.308(a)(6)) **HIPAA Standard:** *Implement policies and procedures to address security incidents.*	

(continued)

4. Develop Recovery Strategy • Finalize the set of contingency procedures that should be invoked for all identified impacts, including emergency mode operation. The strategy must be adaptable to the existing operating environment and address allowable outage times and associated priorities identified in step 2. • Ensure, if part of the strategy depends on external organizations for support, that formal agreements are in place with specific requirements stated.	• IMC:SG4 Escalate Incidents (SP1-SP4) • SC:SG3.SP2 Develop and Document Services Continuity Plans • TM:SG5.SP1 Perform Planning to Sustain Technology Assets • EXD:SG2 Manage Risks Due to External Dependencies (SP1-SP2) • EXD:SG3.SP4 Formalize Relationships
5. Data Backup Plan and Disaster Recovery Plan Implementation Specifications (Both Required) • Establish and implement procedures to create and maintain retrievable exact copies of e-PHI. • Establish (and implement as needed) procedures to restore any loss of data.	• SC:SG3.SP4 Store and Secure Service Continuity Plans • KIM:SG6.SP1 Perform Information Duplication and Retention • KIM:SG6.SP2 Manage Organizational Knowledge
6. Develop and Implement an Emergency Mode Operation Plan Implementation Specification (Required) • Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of e-PHI while operating in emergency mode. • “Emergency mode” operation involves only those critical business processes that must occur to protect the security of e-PHI during and immediately after a crisis situation.	• IMC:SG4 Escalate Incidents (SP1-SP4) • SC:SG1.SP1 Plan for Service Continuity • SC:SG4 Validate Service Continuity Plans (SP1-SP2) • SC:SG6.SP1 Execute Plans

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.6. Security Incident Procedures (C.E.R. § 164.308(a)(6)) **HIPAA Standard:** *Implement policies and procedures to address security incidents.*	
(continued)	
7. Testing and Revision Procedure Implementation Specification (Addressable) • Implement procedures for periodic testing and revision of contingency plans. • Test the contingency plan on a predefined cycle (stated in the policy developed under Key Activity), if reasonable and appropriate. • Train those with defined plan responsibilities on their roles. • If possible, involve external entities (vendors, alternative site/service providers) in testing exercises. • Make key decisions regarding how the testing is to occur ("tabletop" exercise versus staging a real operational scenario including actual loss of capability). • Decide how to segment the type of testing based on the assessment of business impact and acceptability of sustained loss of service. Consider cost.	• SC:SG5 Exercise Service Continuity Plans (SP1-SP4) • SC:GG2.GP5 Train People

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.8. Evaluation (C.E.R. § 164.308(a)(8)) **HIPAA Standard:** *Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.*	
1. Determine Whether Internal or External Evaluation Is Most Appropriate • Decide whether the evaluation will be conducted with internal staff resources or external consultants. • Engage external expertise to assist the internal evaluation team where additional skills and expertise is determined to be reasonable and appropriate. • Use internal resources to supplement an external source of help, because these internal resources can provide the best institutional knowledge and history of internal policies and practices.	• EF:SG4 Provide Resilience Oversight (SP1-SP3) • GG2.GP2 Plan the Process

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.8. Evaluation (C.E.R. § 164.308(a)(8)) **HIPAA Standard:** *Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.*	

(continued)

2. Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule • Use an evaluation strategy and tool that considers all elements of the HIPAA Security Rule and can be tracked, such as a questionnaire or checklist. • Implement tools that can provide reports on the level of compliance, integration, or maturity of a particular security safeguard deployed to protect e-PHI. • If available, consider engaging corporate, legal, or regulatory compliance staff when conducting the analysis. • Leverage any existing reports or documentation that may already be prepared by the organization addressing compliance, integration, or maturity of a particular security safeguard deployed to protect e-PHI.	• COMP:SG1 Prepare for Compliance Management (SP1-SP3) • COMP:SG2 Establish Compliance Obligations (SP1-SP3)
3. Conduct Evaluation • Determine, in advance, what departments and/or staff will participate in the evaluation. • Secure management support for the evaluation process to ensure participation. • Collect and document all needed information. Collection methods may include the use of interviews, surveys, and outputs of automated tools, such as access control auditing tools, system logs, and results of penetration testing. • Conduct penetration testing (where trusted insiders attempt to compromise system security for the sole purpose of testing the effectiveness of security controls), if reasonable and appropriate.	• COMP:SG3 Demonstrate Satisfaction of Compliance Obligations (SP1-SP3) • COMP:GG2.GP2 Plan the Process • COMP:GG2.GG4 Assign Responsibility • COMP:GG2.GP9 Objectively Evaluate Adherence
4. Document Results • Document each evaluation finding, remediation options and recommendations, and remediation decisions. • Document known gaps between identified risks and mitigating security controls, and any acceptance of risk, including justification. • Develop security program priorities and establish targets for continuous improvement.	• COMP:SG3 Demonstrate Satisfaction of Compliance Obligations (SP2-SP3) • COMP:SG4.SP1 Evaluate Compliance Activities • COMP:GG2.GP6 Manage Work Product Configuration • COMP:GG2.GP7 Identify and Involve Relevant Stakeholders

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.8. Evaluation (C.E.R. § 164.308(a)(8)) **HIPAA Standard:** *Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.*	

(continued)

5. Repeat Evaluations Periodically • Establish the frequency of evaluations, taking into account the sensitivity of the e-PHI controlled by the organization, its size, complexity, and environmental and/or operational changes (e.g., other relevant laws or accreditation requirements). • In addition to periodic reevaluations, consider repeating evaluations when environmental and operational changes are made to the organization that affects the security of e-PHI (e.g., if new technology is adopted or if there are newly recognized risks to the security of the information).	• COMP:SG1.SP1-SP3 Prepare for Compliance Management • COMP:SG4.SP1 Monitor Compliance Activities • COMP:GG2.GP8 Monitor And Control the Process • COMP:GG2.GP9 Objectively Evaluate Adherence

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.9. Business Associate Contracts and Other Arrangements (C.E.R. § 164.308(b)(1)) **HIPAA Standard:** *A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information.*	
1. Identify Entities that Are Business Associates under the HIPAA Security Rule • Identify the individual or department who will be responsible for coordinating the execution of business associate agreements or other arrangements. • Reevaluate the list of business associates to determine who has access to e-PHI in order to assess whether the list is complete and current. • Identify systems covered by the contract/agreement.	• EXD:SG1.SP1 Identify External Dependencies • EXD:SG2 Manage Risks Due to External Dependencies • AM:SG1 Manage and Control Access (SP1-SP4) • MON:SG2.SP3 Collect and Record Information

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Administrative Safeguards	
4.9. Business Associate Contracts and Other Arrangements (C.E.R. § 164.308(b)(1)) **HIPAA Standard:** *A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information.*	
(continued)	
2. Written Contract or Other Arrangement Implementation Specification (Required) • Document the satisfactory assurances required by this standard through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a). • Execute new or update existing agreements or arrangements as appropriate. • Identify roles and responsibilities. • Include security requirements in business associate contracts/agreements to address confidentiality, integrity, and availability of e-PHI. • Specify any training requirements associated with the contract/agreement or arrangement, if reasonable and appropriate.	• EXD:SG3 Establish Formal Relationships (SP1-SP4) • EXD:GG2.GP5 Train People
3. Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met • Maintain clear lines of communication. • Conduct periodic security reviews. • Establish criteria for measuring contract performance. • If the business associate is a governmental entity, update the memorandum of understanding or other arrangement when required by law or regulation or when reasonable and appropriate.	• EXD:SG4 Manage External Entity Performance (SP1-SP2)
4. Implement An Arrangement Other than a Business Associate Contract if Reasonable and Appropriate • If the covered entity and its business associate are both governmental entities, use a memorandum of understanding or reliance on law or regulation that requires equivalent actions on the part of the business associate. • Document the law, regulation, memorandum, or other document that assures that the governmental entity business associate will implement all required safeguards for e-PHI involved in transactions between the parties.	• EXD:SG3.SP4 Formalize Relationships • EXD:SG4.SP1 Correct External Entity Performance

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Physical Safeguards	
4.10. Facility Access Controls (C.E.R. § 164.310(a)(1)) **HIPAA Standard:** *Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*	
1. Conduct an Analysis of Existing Physical Security Vulnerabilities • Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities. • Assign degrees of significance to each vulnerability identified and ensure that proper access is allowed. • Determine which types of facilities require access controls to safeguard e-PHI, such as: ◦ Data Centers ◦ Peripheral equipment locations ◦ IT staff offices ◦ Workstation locations.	• EC:SG1.SP1 Prioritize Facility Assets • EC:SG3 Manage Facility Asset Risk (SP1-SP2)
2. Identify Corrective Measures • Identify and assign responsibility for the measures and activities necessary to correct deficiencies and ensure that proper access is allowed. • Develop and deploy policies and procedures to ensure that repairs, upgrades, and /or modifications are made to the appropriate physical areas of the facility while ensuring that proper access is allowed.	• EC:SG2.SP2 Establish and Implement Controls
3. Develop a Facility Security Plan Implementation Specification (Addressable) • Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. • Implement appropriate measures to provide physical security protection for e-PHI in a covered entity's possession. • Include documentation of the facility inventory, as well as information regarding the physical maintenance records and the history of changes, upgrades, and other modifications. • Identify points of access to the facility and existing security controls.	• EC:SG2.SP2 Establish and Implement Controls

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Physical Safeguards	
4.10. Facility Access Controls (C.E.R. § 164.310(a)(1)) **HIPAA Standard:** *Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*	

(continued)

4. Develop Access Control and Validation Procedures Implementation Specification (Addressable) • Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. • Implement procedures to provide facility access to authorized personnel and visitors, and exclude unauthorized persons.	• EC:SG2.SP2 Establish and Implement Controls
5. Establish Contingency Operations Procedures Implementation Specification (Addressable) • Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode • Operations Plan in the event of an emergency.	• EC:SG2.SP1 Assign Resilience Requirements to Facility Assets • EC:SG2.SP2 Establish and Implement Controls • EC:SG4.SP1 Perform Facility Sustainability Planning
6. Maintain Maintenance Records Implementation Specification (Addressable) • Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).	• EC:SG4.SP2 Maintain Environmental Conditions

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Physical Safeguards	
4.11. Workstation Use (C.E.R. § 164.310(b)) **HIPAA Standard:** *Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.*	
1. Identify Workstation Types and Functions or Uses • Inventory workstations and devices. • Develop policies and procedures for each type of workstation and workstation device, identifying and accommodating their unique issues. • Classify workstations based on the capabilities, connections, and allowable activities for each workstation used.	• KIM:SG1.SP1 Prioritize Information Assets • TM:SG1 Prioritize Technology Assets (SP1-SP2)
2. Identify Expected Performance of Each Type of Workstation • Develop and document policies and procedures related to the proper use and performance of workstations.	• KIM:SG1.SP2 Categorize Information Assets • TM:SG1 Prioritize Technology Assets (SP1-SP2)
3. Analyze Physical Surroundings for Physical Attributes • Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts. • Develop policies and procedures that will prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and dispose of sensitive information as needed.	• KIM:SG3.SP1 Identify and Assess Information Asset Risk • TM:SG3.SP1 Identify and Assess Technology Asset Risk

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Physical Safeguards	
4.12. Workstation Security (C.E.R. § 164.310(c)) **HIPAA Standard:** *Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*	
1. Identify All Methods of Physical Access to Workstations • Document the different ways workstations are accessed by employees and nonemployees.	• KIM:SG2.SP1 Establish and Implement Controls • TM:SG2.SP2 Establish and Implement Controls
2. Analyze the Risk Associated with Each Type of Access • Determine which type of access holds the greatest threat to security.	• KIM:SG3.SP1 Identify and Assess Information Asset Risk • TM:SG3.SP1 Identify and Assess Technology Asset Risk

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Physical Safeguards	
4.12. Workstation Security (C.E.R. § 164.310(c)) **HIPAA Standard:** *Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*	
(continued)	
3. Identify and Implement Physical Safeguards for Workstations • Implement physical safeguards and other security measures to minimize the possibility of inappropriate access to e-PHI through workstations.	• KIM:SG2.SP1 Establish and Implement Controls • TM:SG4.SP1 Control Access to Technology Assets

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Physical Safeguards	
4.13. Device and Media Controls (C.E.R. § 164.310(d)(1)) **HIPAA Standard:** *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.*	
1. Implement Methods for Final Disposal of e-PHI Implementation Specification (Required) • Implement policies and procedures to address the final disposition of e-PHI and/or the hardware or electronic media on which it is stored. • Determine and document the appropriate methods to dispose of hardware, software, and the data itself. • Assure that e-PHI is properly destroyed and cannot be recreated.	• KIM:SG4.SP3 Control Information Asset Disposition
2. Develop and Implement Procedures for Reuse of Electronic Media Implementation Specification (Required) • Implement procedures for removal of e-PHI from electronic media before the media are made available for reuse. • Ensure that e-PHI previously stored on electronic media cannot be accessed and reused. • Identify removable media and their use. • Ensure that e-PHI is removed from reusable media before they are used to record new information.	• KIM:SG4.SP3 Control Information Asset Disposition

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Physical Safeguards	
4.13. Device and Media Controls (C.E.R. § 164.310(d)(1)) **HIPAA Standard:** *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.*	

(continued)

3. Maintain Accountability for Hardware and Electronic Media Implementation Specification (Addressable) • Maintain a record of the movements of hardware and electronic media and any person responsible therefore. • Ensure that e-PHI is not inadvertently released or shared with any unauthorized party. • Ensure that an individual is responsible for, and records the receipt and removal of, hardware and software with e-PHI.	• KIM:SG4.SP3 Control Information Asset Disposition • KIM:SG6.SP1 Perform Information Duplication and Retention • KIM:SG6.SP2 Manage Organization Knowledge
4. Develop Data Backup and Storage Procedures Implementation Specification (Addressable) • Create a retrievable exact copy of e-PHI, when needed, before movement of equipment. • Ensure that an exact retrievable copy of the data is retained and protected to protect the integrity of e-PHI during equipment relocation.	• KIM:SG6.SP1 Perform Information Duplication and Retention

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.14. Access Control (C.E.R. § 164.312(a)(1)) **HIPAA Standard:** *Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).*	
1. Analyze Workloads and Operations To Identify the Access Needs of All Users • Identify an approach for access control. • Consider all applications and systems containing e-PHI that should be available only to authorized users. • Integrate these activities into the access granting and management process.	• TM:SG4.SP1.Control Access to Technology Assets • KIM:SG4.SP2 Control Access to Information Assets
2. Identify Technical Access Control Capabilities • Determine the access control capability of all information systems with e-PHI.	• AM:SG1 Manage and Control Access (SP1-SP4) • TM:SG2.SP2 Establish and Implement Controls

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.14. Access Control (C.E.R. § 164.312(a)(1)) **HIPAA Standard:** *Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).*	

(continued)

3. Ensure that All System Users Have Been Assigned a Unique Identifier Implementation Specification (Required) • Assign a unique name and/or number for identifying and tracking user identity. • Ensure that system activity can be traced to a specific user. • Ensure that the necessary data is available in the system logs to support audit and other related business functions.	• ID:SG1 Establish Identities (SP1-SP3)
4. Develop Access Control Policy • Establish a formal policy for access control that will guide the development of procedures. • Specify requirements for access control that are both feasible and cost-effective for implementation.	• TM:SG2.SP1 Assign Resilience Requirements to Technology Assets • TM:SG4.SP1 Control Access to Technology Assets • AM:SG1 Manage and Control Access (SP1-SP4)
5. Implement Access Control Procedures Using Selected Hardware and Software • Implement the policy and procedures using existing or additional hardware/software solution(s).	• TM:SG2.SP2 Establish and Implement Controls • KIM:SG2.SP2 Establish and Implement Controls
6. Review and Update User Access • Enforce policy and procedures as a matter of ongoing operations. • Determine if any changes are needed for access control mechanisms. • Establish procedures for updating access when users require the following: ◦ Initial access ◦ Increased access ◦ Access to different systems or applications than those they currently have	• AM:SG1 Manage and Control Access (SP2-SP3)
7. Establish an Emergency Access Procedure Implementation Specification (Required) • Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. • Identify a method of supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems.	• AM:SG1.SP2 Manage Change to Access Privileges

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.14. Access Control (C.E.R. § 164.312(a)(1)) **HIPAA Standard:** *Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).*	

(continued)

8. Automatic Logoff and Encryption and Decryption Implementation Specifications (Both Addressable) • Consider whether the addressable implementation specifications of this standard are reasonable and appropriate: ◦ Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. ◦ Implement a mechanism to encrypt and decrypt e-PHI.	• KIM:SG4.SP1 Encrypt High-Value Information • KIM:SG4.SP2 Control Access to Information Assets
9. Terminate Access if it is No Longer Required • Ensure that access to e-PHI is terminated if the access is no longer authorized.	• HRM:SG4.SP2 Manage Access to Assets • AM:SG1 Manage and Control Access (SP2-SP3)

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.15. Audit Controls (C.E.R. § 164.312(b)) **HIPAA Standard:** *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*	
1. Determine the Activities that Will Be Tracked or Audited • Determine the appropriate scope of audit controls that will be necessary in information systems that contain or use e-PHI based on the covered entity's risk assessment and other organizational factors. • Determine what data needs to be captured.	• CTRL:SG1.SP1 Define Control Objectives • COMP:SG2.SP1 Identify Compliance Obligations
2. Select the Tools that Will Be Deployed for Auditing and System Activity Reviews • Evaluate existing system capabilities and determine if any changes or upgrades are necessary.	• CTRL:SG4 Assess Control Effectiveness • CTRL:GG2.GP3 Provide Resources

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.15. Audit Controls (C.E.R. § 164.312(b)) **HIPAA Standard:** *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*	

(continued)

3. Develop and Deploy the Information System Activity Review/Audit Policy • Document and communicate to the workforce the facts about the organization's decisions on audits and reviews.	• ALL of CTRL Process Area
4. Develop Appropriate Standard Operating Procedures • Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports.	• ALL of CTRL Process Area
5. Implement the Audit/System Activity Review Process • Activate the necessary audit system. • Begin logging and auditing procedures.	• CTRL:SG4 Assess Control Effectiveness

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.16. Integrity (C.E.R. § 164.312(c)(1)) **HIPAA Standard:** *Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.*	
1. Identify All Users Who Have Been Authorized to Access e-PHI • Identify all approved users with the ability to alter or destroy data, if reasonable and appropriate. • Address this Key Activity in conjunction with the identification of unauthorized sources in Key Activity 2, below.	• ID:SG1.SP2 Establish Identity Community
2. Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify It • Identify scenarios that may result in modification to the e-PHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors). • Conduct this activity as part of your risk analysis.	• KIM:SG3.SP1 Identify and Assess Information Asset Risk • ID:SG2.SP2 Monitor and Manage Identity Changes

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.16. Integrity (C.E.R. § 164.312(c)(1)) **HIPAA Standard:** *Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.*	
(continued)	
3. Develop the Integrity Policy and Requirements • Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps.	• ID:SG2.SP3 Correct Inconsistencies
4. Implement Procedures to Address These Requirements • Identify and implement methods that will be used to protect the information from modification. • Identify and implement tools and techniques to be developed or procured that support the assurance of integrity.	• ID:SG2.SP3 Correct Inconsistencies
5. Implement a Mechanism to Authenticate e-PHI Implementation Specification (Addressable) • Implement electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner. • Consider possible electronic mechanisms for authentication such as: ◦ Error-correcting memory ◦ Magnetic disk storage ◦ Digital signatures ◦ Check sum technology.	• KIM:SG5.SP1 Control Modification to Information Assets • TM:SG4.SP1 Control Access to Technology Assets
6. Establish a Monitoring Process To Assess How the Implemented Process Is Working • Review existing processes to determine if objectives are being addressed. • Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised.	• KIM:SG5.SP1 Control Modification to Information Assets • KIM:GG2.GP8 Monitor and Control the Process • TM:SG4.SP1 Control Access to Technology Assets • TM:GG2.GP8 Monitor and Control the Process

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.17. Person or Entity Authentication (C.E.R. § 164.312(d)) **HIPAA Standard:** *Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.*	
1. Determine Authentication Applicability to Current Systems/Applications • Identify methods available for authentication. Under the HIPAA Security Rule, authentication is the corroboration that a person is the one claimed. (45 CFR § 164.304). • Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that he or she has been authorized for specific access privileges to information and information systems.	• KIM:SG2.SP2 Establish and Implement Controls • KIM:SG4.SP1 Encrypt High-Value Information
2. Evaluate Authentication Options Available • Weigh the relative advantages and disadvantages of commonly used authentication approaches. • There are four commonly used authentication approaches available: ◦ Something a person knows, such as a password, ◦ Something a person has or is in possession of, such as a token (smart card, ATM card, etc.), ◦ Some type of biometric identification a person provides, such as a fingerprint, or ◦ A combination of two or more of the above approaches.	• KIM:SG2.SP2 Establish and Implement Controls • KIM:SG4.SP1 Encrypt High-Value Information
3. Select and Implement Authentication Option • Consider the results of the analysis conducted under Key Activity 2, above, and select appropriate authentication methods. • Implement the methods selected into your operations and activities	• KIM:SG2.SP2 Establish and Implement Controls • KIM:SG4.SP1 Encrypt High-Value Information

NIST SP 800-66 Key Activities and Description	CERT-RMM Mapping
Technical Safeguards	
4.18. Transmission Security (C.E.R. § 164.312(e)(1)) **HIPAA Standard:** *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*	
1. Identify Any Possible Unauthorized Sources that May Be Able to Intercept and/or Modify the Information • Identify scenarios that may result in modification of the e-PHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors).	• KIM:SG3.SP1 Identify and Assess Information Asset Risk • KIM:SG5.SP1 Control Modification of Information Assets
2. Develop and Implement Transmission Security Policy and Procedures • Establish a formal (written) set of requirements for transmitting e-PHI. • Identify methods of transmission that will be used to safeguard e-PHI. • Identify tools and techniques that will be used to support the transmission security policy. • Implement procedures for transmitting e-PHI using hardware and/or software, if needed.	• KIM:SG4.SP1 Encrypt High-Value Information • KIM:SG5.SP1 Control Modification of Information Assets • KIM:GG2.GP1 Establish Process Governance
3. Implement Integrity Controls Implementation Specification (Addressable) • Implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without detection until disposed of.	• KIM:SG5.SP1 Control Modification of Information Assets
4. Implement Encryption Implementation Specification (Addressable) • Implement a mechanism to encrypt e-PHI whenever deemed appropriate.	• KIM:SG4.SP1 Encrypt High-Value Information

Bibliography

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

[Allen 2010]
Allen, Julia H.; Caralli, Richard H.; & White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience.* Addison-Wesley Professional, 2010.

[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

[Scholl 2008]
Scholl, Matthew; Stine, Kevin; Hash, Joan; Bowen, Pauline; Johnson, Arnold; Smith, Carla Dancy; & Steinberg, Daniel I. *NIST Special Publication 800-66 Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.* National Institute of Standards and Technology (NIST), 2008.
http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	October 2013	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication 800-66 Crosswalk	FA8721-05-C-0003

6. AUTHOR(S)

Lisa R. Young, Ma-Nyahn Kromah

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-TN-027

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

Organizations can use the CERT® Resilience Management Model (CERT®-RMM) V1.1, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute, to determine how their current practices can support their level of process maturity in areas of operational resilience (business continuity, disaster recovery, management and security planning, and IT operations and service delivery). This technical note is a follow-on to the *CERT-RMM Code of Practice Crosswalk, Commercial Version 1.1* (CMU/SEI-2011-TN-012) and connects CERT-RMM process areas to *NIST Special Publication 800-66 Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Health Insurance Portability and Accountability Act, HIPAA, CERT Resilience Management Model, CERT-RMM, National Institute of Standards and Technology, NIST	43

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