Implementing the HIPAA Security Rule: Special Publication 800-66

Safeguarding Health Information:
Building Assurance through HIPAA Security

A CMS – NIST Conference
May 19, 2009

Kevin Stine
Computer Security Division
National Institute of Standards and Technology

NIST Special Publication 800-26

NIST
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Security Self-Assessment Guide
for Information Technology
Systems

Marianne Swanson

COMPUTER SECURITY

NIST Publications Support the HIPAA Security Rule

Some Security Rule Standards	Some Relevant NIST Publications
Security Management Process (RA, RM)	SP 800-30, 800-37, 800-53
Access Control	SP 800-63
Security Awareness & Training	SP 800-16, 800-50, 800-53
Contingency Planning	SP 800-34, 800-53
Evaluation	SP 800-37, 800-53, 800-53A
Device & Media Controls	SP 800-53, 800-88, 800-111
Transmission Security (Encryption)	FIPS 140-2, SP 800-97, 800-113

What is Special Publication (SP) 800-66?

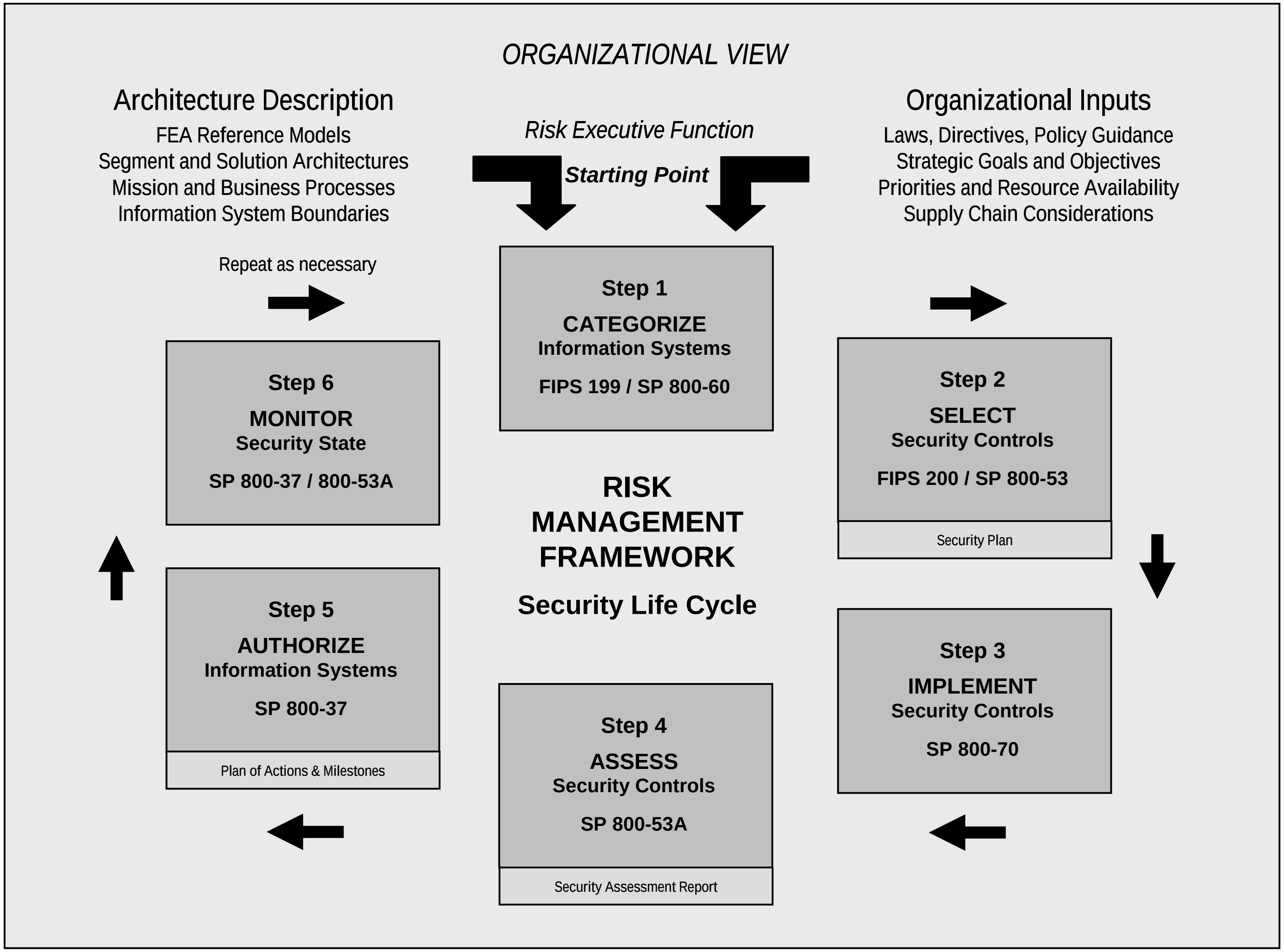
An Introductory Resource Guide for Implementing the HIPAA Security Rule

- Updated October 2008
- Intended as an aid to understanding security concepts discussed in the HIPAA Security Rule
- Directs readers to NIST publications relevant to topics addressed by the Security Rule
- <u>Does not supplement, replace, or supersede the HIPAA Security Rule itself</u>

Why We Updated 800-66?

- To reflect current NIST resources and publications
- To discuss the latest threats, vulnerabilities, and exposures, as well as the technologies used to combat them
- To propose methodologies covered entities may use to tackle specific Security Rule implementation challenges (ex, Risk Assessment, Contingency Planning)
- To set the stage, through security control mappings, for security automation of technical safeguards

NIST Risk Management Framework (RMF)



ORGANIZATIONAL VIEW

Architecture Description

FEA Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Risk Executive Function

Starting Point

Organizational Inputs

Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60

Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53
Security Plan

Step 3
IMPLEMENT
Security Controls
SP 800-70

Step 4
ASSESS
Security Controls
SP 800-53A
Security Assessment Report

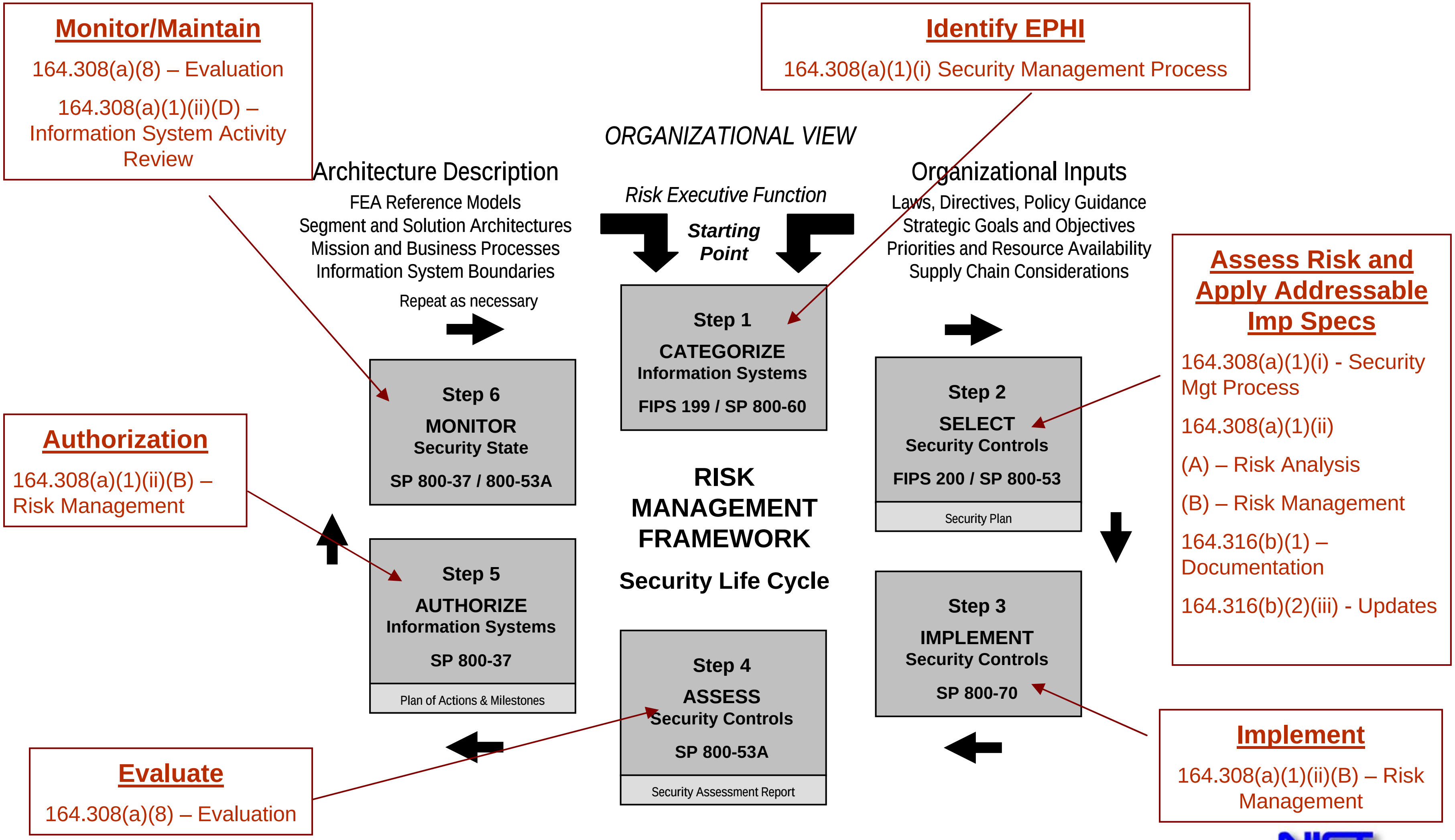
Step 5
AUTHORIZE
Information Systems
SP 800-37
Plan of Actions & Milestones

Step 6
MONITOR
Security State
SP 800-37 / 800-53A

RISK MANAGEMENT FRAMEWORK

Security Life Cycle

Applying the Security Rule to the RMF



Monitor/Maintain

164.308(a)(8) – Evaluation

164.308(a)(1)(ii)(D) – Information System Activity Review

Identify EPHI

164.308(a)(1)(i) Security Management Process

ORGANIZATIONAL VIEW

Architecture Description

FEA Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Risk Executive Function

Starting Point

Organizational Inputs

Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60

Step 6
MONITOR
Security State
SP 800-37 / 800-53A

Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53
Security Plan

Assess Risk and Apply Addressable Imp Specs

164.308(a)(1)(i) - Security Mgt Process

164.308(a)(1)(ii)

(A) – Risk Analysis

(B) – Risk Management

164.316(b)(1) – Documentation

164.316(b)(2)(iii) - Updates

Authorization

164.308(a)(1)(ii)(B) – Risk Management

RISK MANAGEMENT FRAMEWORK

Security Life Cycle

Step 5
AUTHORIZE
Information Systems
SP 800-37
Plan of Actions & Milestones

Step 4
ASSESS
Security Controls
SP 800-53A
Security Assessment Report

Step 3
IMPLEMENT
Security Controls
SP 800-70

Implement

164.308(a)(1)(ii)(B) – Risk Management

Evaluate

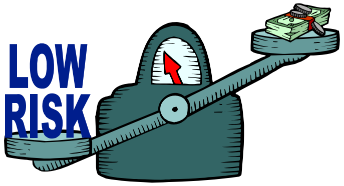
164.308(a)(8) – Evaluation

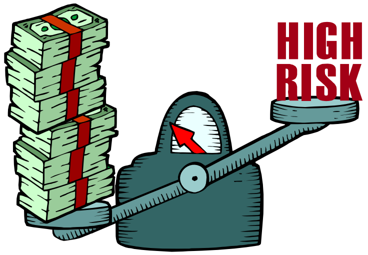
Risk Assessment Guidelines

- Provide basic strategies to help covered entities identify and mitigate risks to acceptable levels

- Discuss the role of risk assessment in enterprise risk management

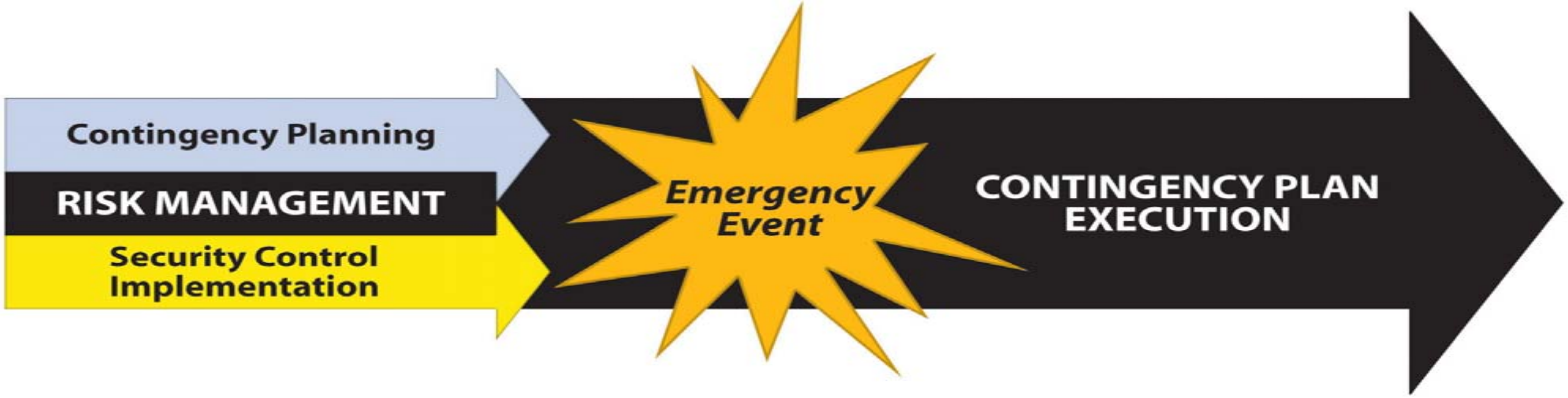
- Propose a methodology for conducting a risk assessment





Contingency Planning Guidelines

- Identify basic contingency planning principles and practices
- Discuss its role in a risk management process
- Discuss scope of different types of contingency plans
- Propose a process for developing and maintaining a contingency plan, and provide a sample template



NIST
National Institute of Standards and Technology

Special Considerations

- Key Activities typically associated with each Security Rule standard

- Strategies and Considerations for Secure Remote Use and Access

Setting the Stage for Automation:
NIST Security Controls Support the Security Rule

Section of HIPAA Security Rule	HIPAA Security Rule Standards	Implementation Specifications	NIST SP 800-53 Security Controls Mapping	NIST Publications Crosswalk
164.312(a)(2)(iii)		Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	AC-11, AC-12	
164.312(a)(2)(iv)		Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information.	AC-3, SC-13	
164.312(b)	Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.		AU-1, AU-2, AU-3, AU-4, AU-6, AU-7	NIST SP 800-12 NIST SP 800-14 NIST SP 800-42 NIST SP 800-53 NIST SP 800-53A NIST SP 800-55 NIST SP 800-92 NIST SP 800-115
164.312(c)(1)	Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.		CP-9, MP-2, MP-5, SC-8, SI-1, SI-7	NIST SP 800-12 NIST SP 800-14 NIST SP 800-53 NIST Draft SP 800-106 NIST Draft SP 800-107
164.312(c)(2)		Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	SC-8, SI-7	
164.312(d)	Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.		IA-2, IA-3, IA-4	FIPS 201 NIST SP 800-12 NIST SP 800-14 NIST SP 800-53 NIST SP 800-63