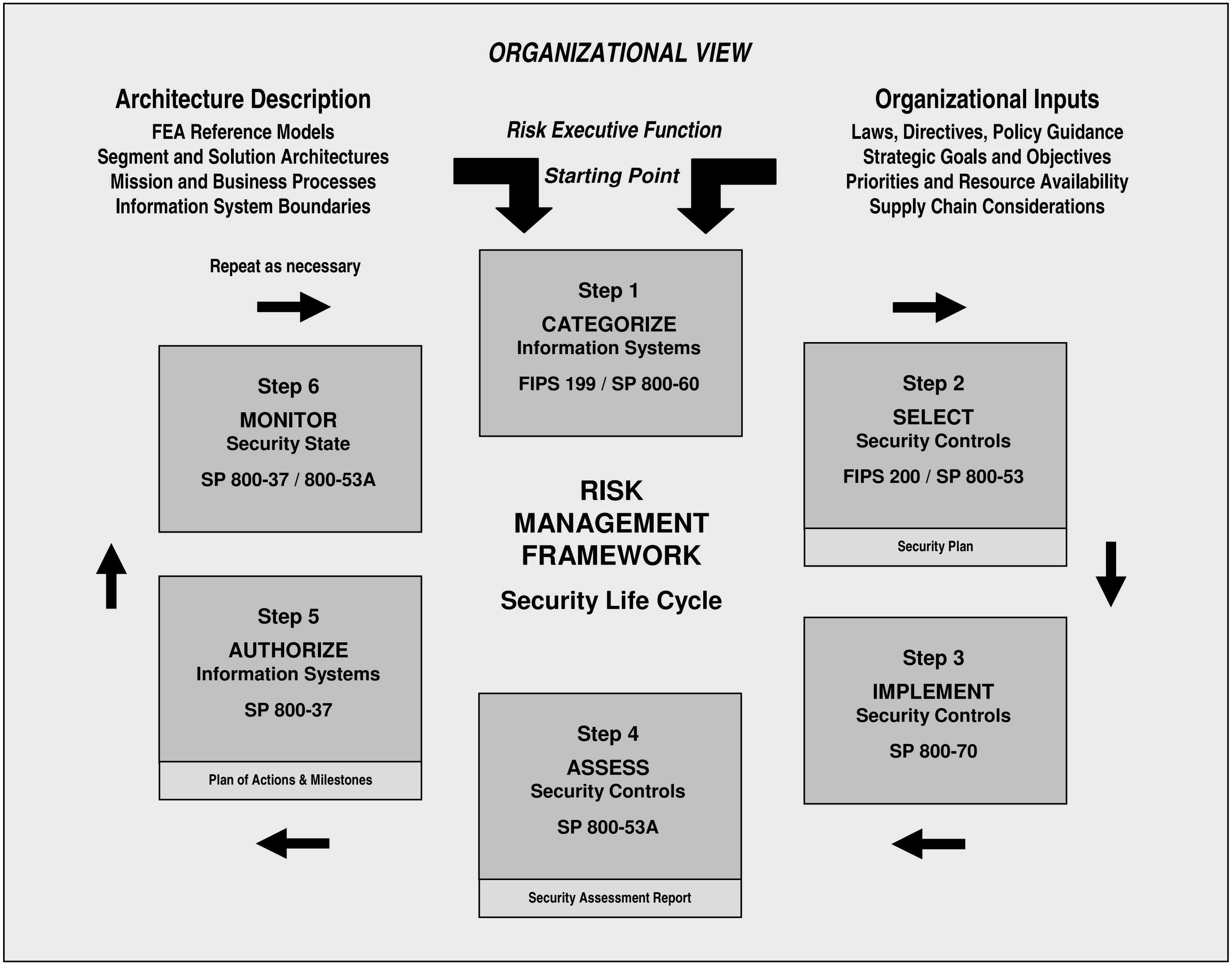
What is SP 800-66?

- An Introductory Resource Guide for Implementing the HIPAA Security Rule
  - Originally published in March 2005
  - 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
  - Does not supplement, replace, or supersede the HIPAA Security Rule itself

NIST Risk Management Framework



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

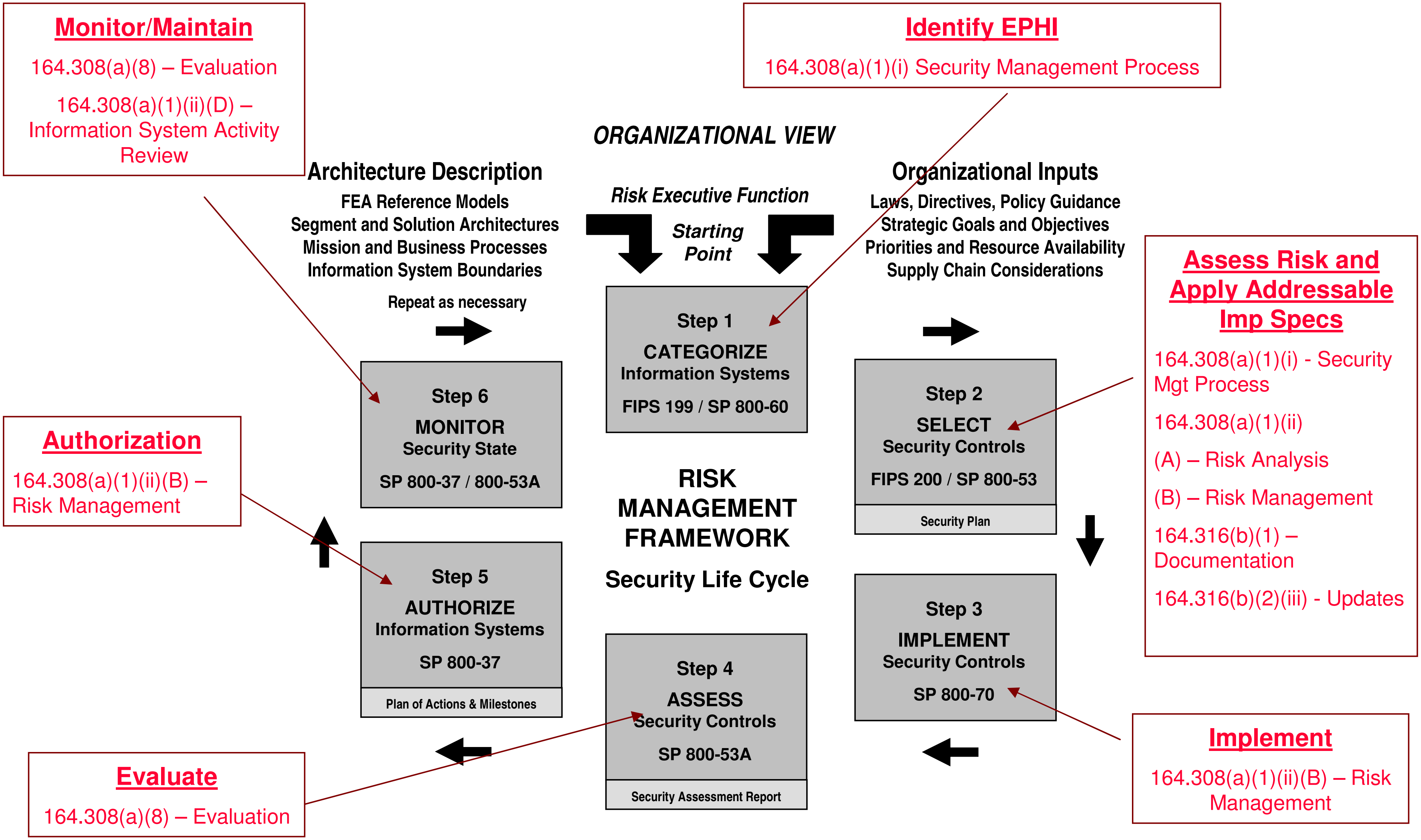
Step 5
AUTHORIZE
Information Systems
SP 800-37
Plan of Actions & Milestones

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

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

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

Authorization

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

Implement

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

Evaluate

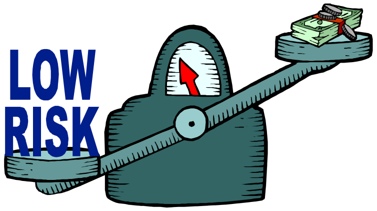
164.308(a)(8) – Evaluation

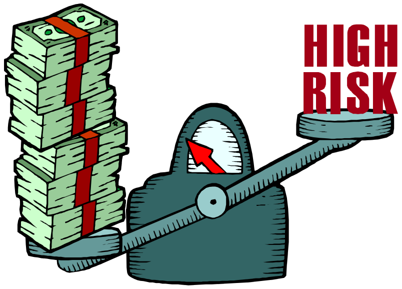
Risk Assessment Guidelines

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

- Discuss the role of risk assessment in enterprise risk management

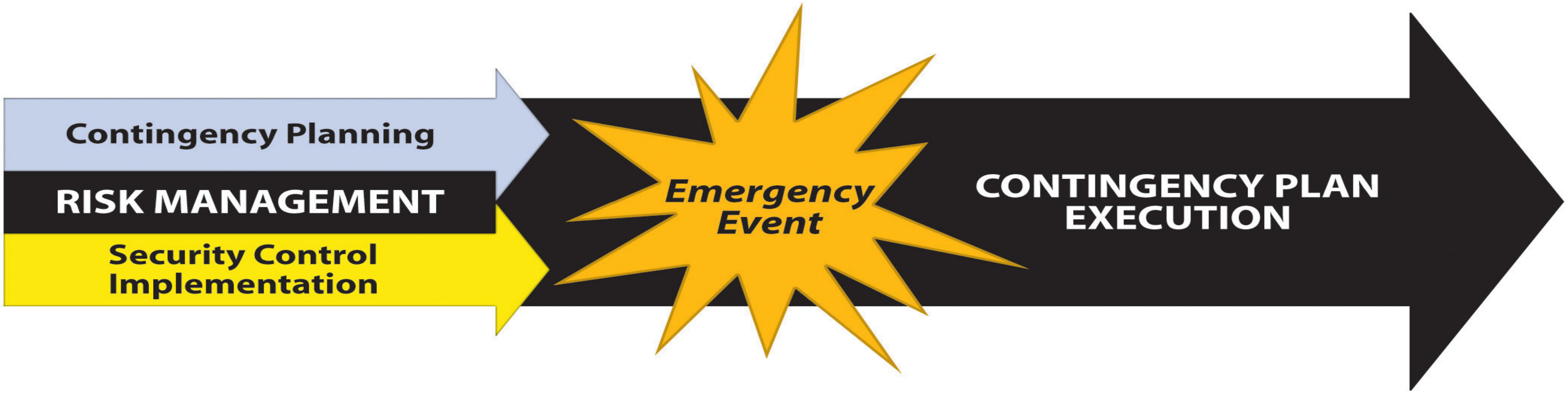
- Propose a methodology for conducting a risk assessment





Contingency Planning Guidelines

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


Contingency Planning

RISK MANAGEMENT

Security Control Implementation

Emergency Event

CONTINGENCY PLAN EXECUTION

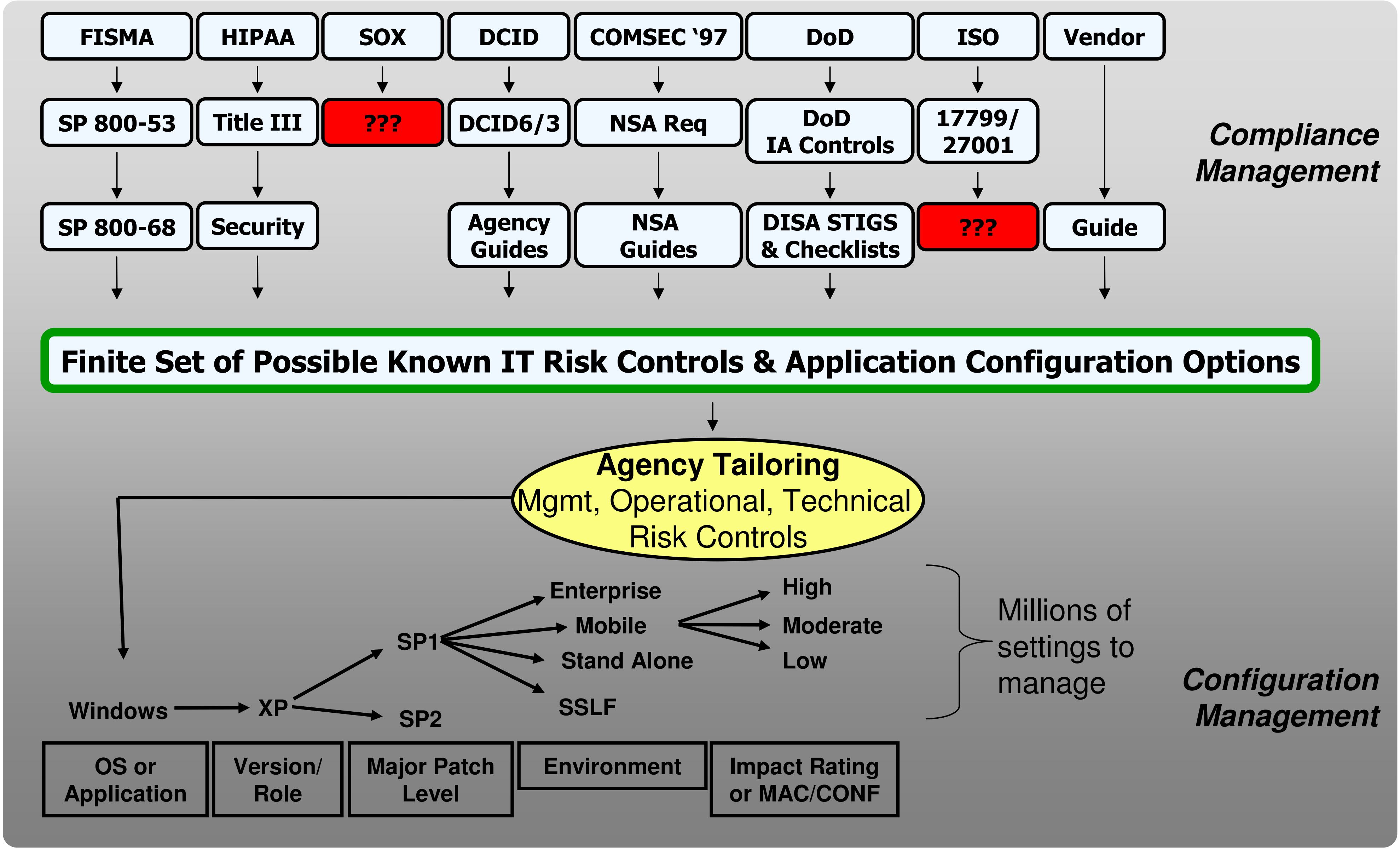
Special Considerations and Resources

- Key Activities typically associated with each Security Rule standard

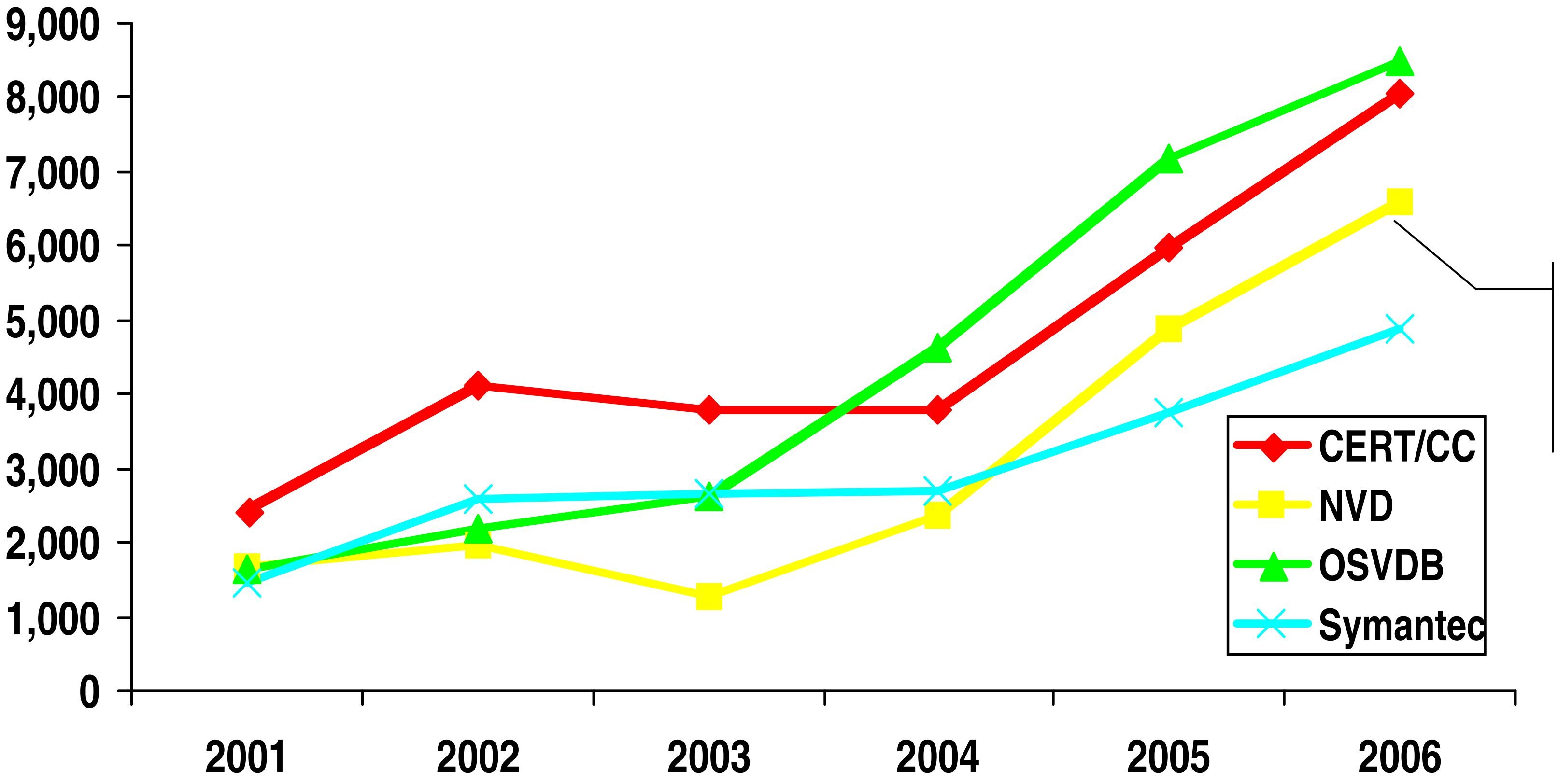
- Remote Use and Access

- Storage and Removable Media Protections

Current State: Compliance and Configuration Management



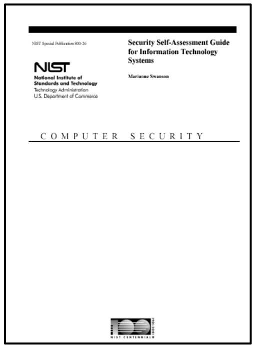
Current State: Vulnerability Trends



A 20-50% increase over previous years

- Decreased timeline in exploit development
- Increased prevalence of zero day exploits
- Three of the SANS Top 20 Internet Security Attack Targets 2006 were categorized as “configuration weaknesses.” Many of the remaining 17 can be partially mitigated via proper configuration.

NIST Publications Support the HIPAA Security Rule



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 CENTENNIAL

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 (Draft)
Device & Media Controls	SP 800-88, 800-53, 800-34
Transmission Security (Encryption)	FIPS 140-2, SP 800-113, 800-97

NIST Controls Support the HIPAA 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 Draft SP 800-53A NIST SP 800-55 NIST SP 800-92 NIST Draft 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

Existing Federal Content

Standardizing What We Communicate

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

- In response to NIST being named in the Cyber Security R&D Act of 2002
- Encourages vendor development and maintenance of security guidance
- Currently hosts 114 separate guidance documents for over 141 IT products
- Translating this backlog of checklists into the Security Content Automating Protocol (SCAP)
- Participating organizations: DISA, NSA, NIST, Hewlett-Packard, CIS, ITAA, Oracle, Sun, Apple, Microsoft, Citadel, LJK, Secure Elements, ThreatGuard, MITRE Corporation, G2, Verisign, Verizon Federal, Kyocera, Hewlett-Packard, ConfigureSoft, McAfee, etc.

Sponsored by DHS National Cyber Security Division/US-CERT

National Vulnerability Database

a comprehensive cyber vulnerability resource

NIST National Institute of Standards and Technology

- Over 70 million hits per year
- 29,000 vulnerabilities; about 20 new per day
- Mis-configuration cross references to:
  - NIST SP 800-53 Security Controls (All 17 Families and 163 controls)
  - DoD IA Controls
  - DISA VMS Vulnerability IDs
  - Gold Disk VIDs
  - DISA VMS PDI IDs
  - NSA References
  - DCID
  - ISO 17799
- Reconciles software flaws from:
  - US CERT Technical and Vulnerability Alerts
  - MITRE OVAL Software Flaw Checks
  - MITRE CVE Dictionary
- Produces XML feed for NVD content

Summary

- SCAP gives us a transparent, interoperable, repeatable, and ultimately automated way to assess security software flaws and misconfigurations in the enterprise
- Efficiencies gained through SCAP give our IT security teams additional cycles to address other important aspects of IT security
- By linking compliance to configuration, SCAP makes compliance reporting a byproduct of good security, allowing IT security teams to focus on securing the enterprise