CYA with NIST (National Institute of Standards and Technology) Security Standards on System z

Presented by

Brian J. Marshall

VP Research and Development

Trademarks

- The following are trademarks or registered trademarks of the International Business Machines Corporation:
  - IBM Logo
  - z/OS
  - MVS/ESA
  - S/390
  - DB2

  - OS/390
  - MVS/DFP
  - RACF
  - Series z
  - IBM Business Partner emblem
- UNIX is a registered trademark of The Open Group in the United States and other countries.

Agenda

Terminology

The NIST Standards

The NIST Risk Management Framework

The NVD and NCP

Questions

Terminology

DISA: Defense Information Systems Agency

DoD: Department of Defense

NIST: National Institute of Standards and Technology

FIPS: Federal Information Processing Standard (Required Standards)

FISMA: Federal Information Security Management Act of 2002 (Eliminated Waivers)

SP: Special Publications (Guideline)

SRR: Security Readiness Review – the audit performed using the DISA STIGs.

STIG: Security Technical Implementation Guide

NVD: National Vulnerability Database

NCP: National Checklist program

The NIST STANDARDS by FAMILY

Access Control	**FIPS 200 and 201**
	SP 800-53
Audit & Accountability	**FIPS 200**
	SP 800-137
Awareness & Training	**FIPS 200**
	SP 800-53
	SP 800-50
Certification, Accreditation & Security Assessments	**FIPS 200**
	SP 800-126
	SP 800-117
Configuration Management	**FIPS 200**
	SP 800-126
	SP 800-53
Contingency Planning	**FIPS 200**

The NIST STANDARDS by FAMILY

Identification & Authentication	**FIPS 201**
	FIPS 200
	SP 800-53
Incident Response	**FIPS 200**
	SP 800-126
Maintenance	**FIPS 200**
	SP 800-126
	SP 800-53
Media Protection	**FIPS 200**
	SP 800-124
	SP 800-53
Personnel Security	**FIPS 200**
	SP 800-53

The NIST STANDARDS by FAMILY

Physical & Environmental Protection	**FIPS 200**
	SP 800-123
Planning	**FIPS 201**
	FIPS 200
	SP 800-153
Risk Assessment	**FIPS 199**
	FIPS 200
	SP 800-53
	SP 800-137
System & Communications Protection	**FIPS 197** **FIPS 198**
	FIPS 200
	FIPS 201

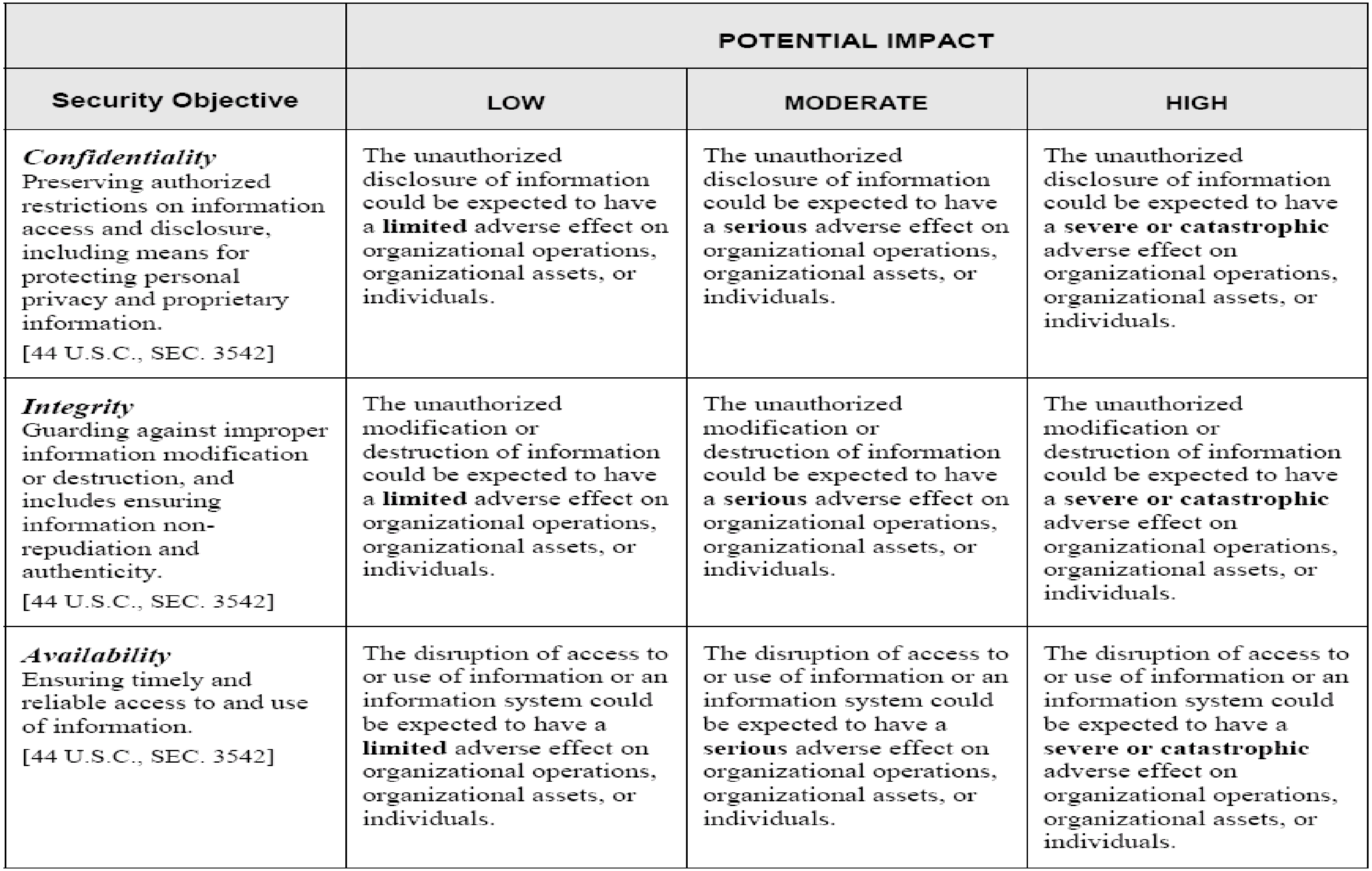
The NIST STANDARDS by FAMILY

Physical & Environmental Protection	FIPS 200
	SP 800-123
Planning	FIPS 201
	FIPS 200
	SP 800-153
Risk Assessment	FIPS 199
	FIPS 200
	SP 800-53
	SP 800-137
System & Communications Protection	FIPS 200
	FIPS 201

The NIST STANDARDS by FAMILY

System & Information Integrity	FIPS 200
	FIPS 140
	SP 800-53
System & Services Acquisition	FIPS 200
	SP 800-147

FIPS 199



	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

FIPS 200

Outlines the specification for Minimum Security Requirements (17 categories)

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Certification, Accreditation, and Security Assessments (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA):

FIPS 200

- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

FIPS 200

- **Access Control (AC):** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
- **Awareness and Training (AT):** Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- **Audit and Accountability (AU):** Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
- **Certification, Accreditation, and Security Assessments (CA):** Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- **Configuration Management (CM):** Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

FIPS 200

- **Contingency Planning (CP):** Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
- **Identification and Authentication (IA):** Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- **Incident Response (IR):** Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
- **Maintenance (MA):** Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- **Media Protection (MP):** Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.
- **Physical and Environmental Protection (PE):** Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
- **Planning (PL):** Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

FIPS 200

- **Personnel Security (PS):** Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
- **Risk Assessment (RA):** Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
- **System and Services Acquisition (SA):** Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
- **System and Communications Protection (SC):** Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
- **System and Information Integrity (SI):** Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

FIPS 201 and HSPD-12

FIPS 201 (**Federal Information Processing Standard** **Publication 201**) is a United States federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors.

In response to HSPD-12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201 was developed to satisfy the technical requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005.

FIPS 201 together with NIST SP 800-78 (Cryptographic Algorithms and Key Sizes for PIV) are required for U.S. Federal Agencies,

NIST SP 800-53 R3 and FIPS 200

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to FISMA.

FIPS 200 and NIST Special Publication 800-53, in combination, help ensure that appropriate security requirements and security controls are applied to all federal information and information systems. An organizational assessment of risk validates the initial security control selection and determines if any additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of security due diligence for the organization.

Of the eighteen security control families in NIST Special Publication 800-53, seventeen families are described in the security control catalog, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS 200. One additional family (Program Management [PM] family) provides controls for information security programs. This family, while not referenced in FIPS 200, provides security controls at the organizational rather than the information-system level.

NIST SP 800-53 R3

Purpose of NIST SP 800-53: The purpose of NIST 800-53 is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations.

Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;

Providing a stable, yet flexible catalog of security controls for information systems and organizations to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies;

Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness; and

Improving communication among organizations by providing a common lexicon that supports discussion of risk management concepts.

NIST SP 800-53 R3 Process

Select and Specify security controls for an information system including:

(i) applying the organization’s overall approach to managing risk;

(ii) categorizing the information system and determining the system impact level in accordance with FIPS 199 and FIPS 200, respectively;

(iii) selecting the initial set of baseline security controls, tailoring the baseline controls, and supplementing the tailored baseline, as necessary, in accordance with an organizational assessment of risk; and

(iv) assessing the security controls as part of a comprehensive continuous monitoring process.

NIST 800-37

NIST 800-37 is the publication that describes the tasks required to apply the Risk Management Framework to information systems including:

(i) the categorization of information and information systems;

(ii) the selection of security controls;

(iii) the implementation of security controls;

(iv) the assessment of security control effectiveness;

(v) the authorization of the information system;

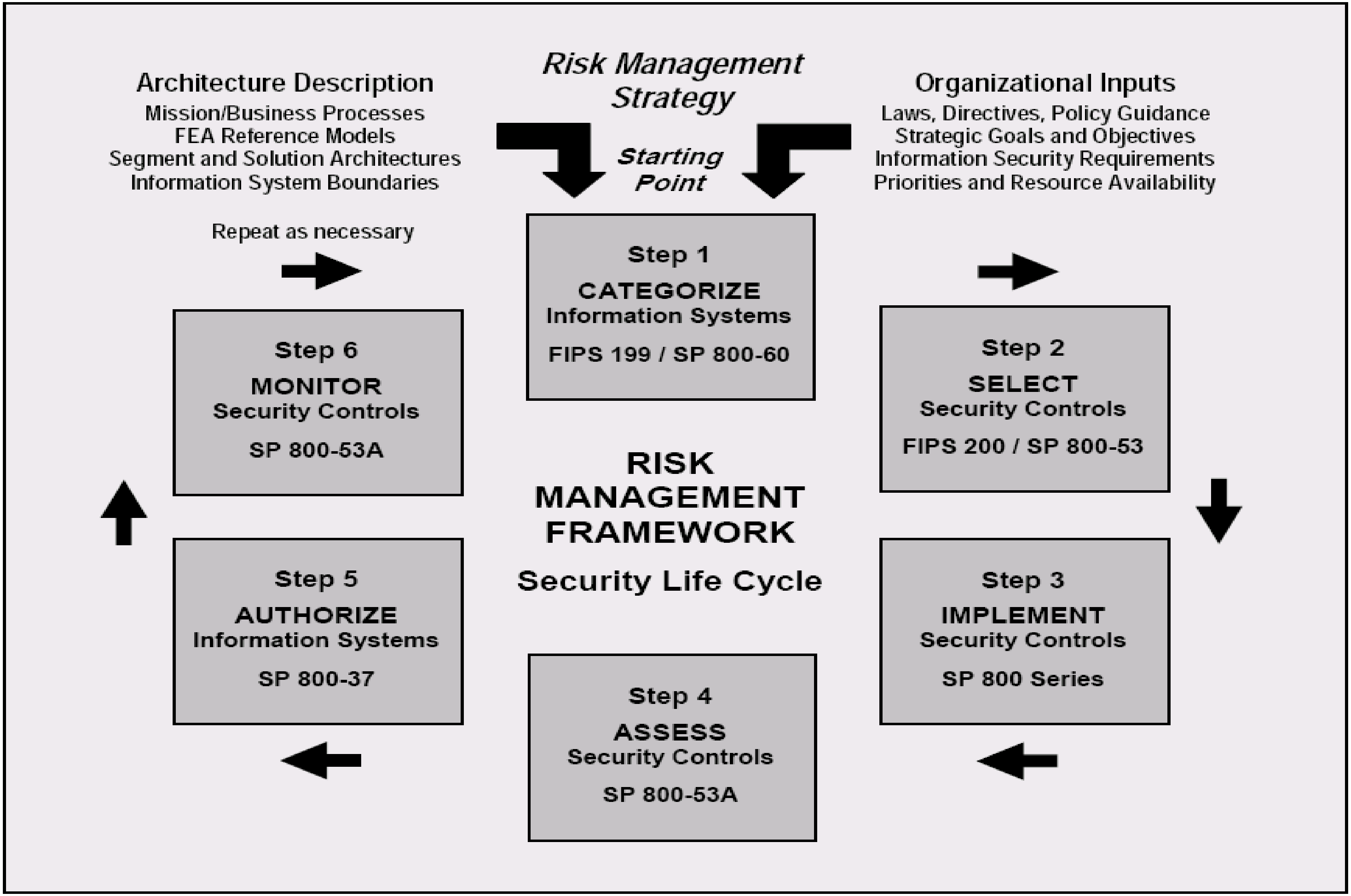
(vi) the ongoing monitoring of security controls and the security state of the information system.

NIST SP 800-137

Establishes that their must be Ongoing Monitoring in Support of Risk Management.

It specifically addresses assessment and analysis of security control effectiveness and of organizational security status in accordance with organizational risk tolerance.

NIST Risk Management Framework



Risk Management Strategy

Starting Point

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

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Information Security Requirements
Priorities and Resource Availability

Repeat as necessary

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

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

Step 3
IMPLEMENT
Security Controls
SP 800 Series

Step 4
ASSESS
Security Controls
SP 800-53A

Step 5
AUTHORIZE
Information Systems
SP 800-37

Step 6
MONITOR
Security Controls
SP 800-53A

RISK MANAGEMENT FRAMEWORK

Security Life Cycle

NIST Risk Management Framework

FIPS 199: Identify potential impact of security objectives.

FIPS 200: Outline of Minimum Security Requirements

NIST SP 800-53A: Covers both the security control assessment and continuous monitoring steps in the Risk Management Framework.

NIST SP 800-53: Outlines the steps in the Risk Management Framework that address security control selection.

NIST SP 800-37: Companion document to 800-53 that specifies the assessment procedures and the guidelines for developing security assessment plans and continuous monitoring

NIST 800-53 rev 3 process

Categorize the information system and the information processed, stored, and transmitted by that system based on a FIPS 199 impact analysis.

Select an initial set of baseline security controls for the information system based on the system impact level and minimum security requirements defined in FIPS 200;

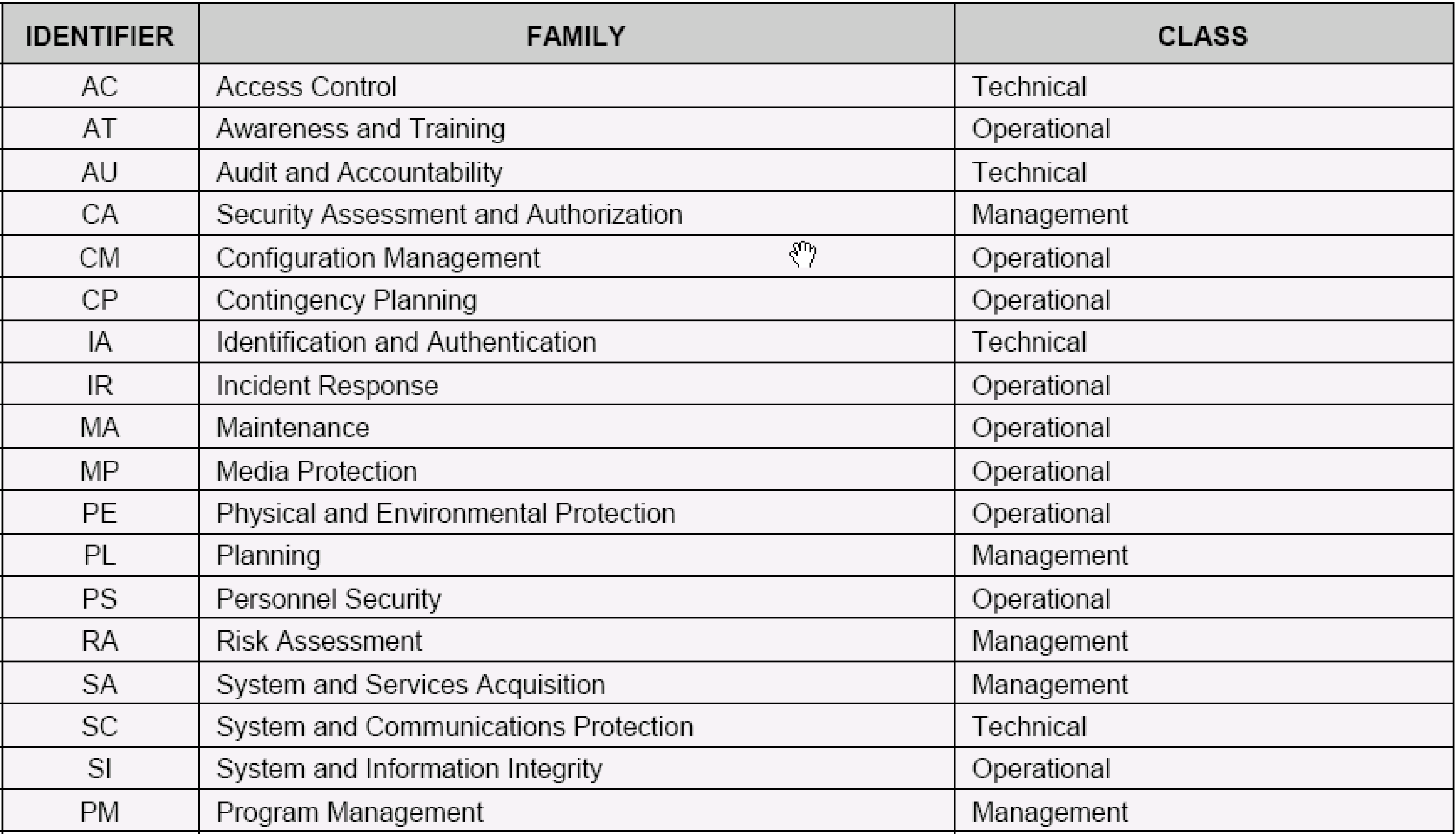
Implement the security controls and describe how the controls are employed within the information system and its environment of operation

Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

NIST 800-53 R3 Security Control Classes



IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

NIST 800-53A

NIST SP 800-53A is a companion guideline to NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.

NIST SP 800-53 covers the steps in the Risk Management Framework that address security control selection while NIST Special Publication 800-53A covers both the security control assessment and continuous monitoring steps in the Risk Management Framework and provides guidance on the security assessment process.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* is a companion document to 800-53 that specifies the assessment procedures and the guidelines for developing security assessment plans and continuous monitoring

NIST 800-60

Contains the basic guidelines for mapping types of information and information systems to security categories. The appendices, including security categorization recommendations for mission-based information types and rationale for security categorization recommendations, are published as a separate Volume II.

NIST 800-126

NIST 800-126 is the Technical Specifications for the Security Content Automation Protocol

NVD and NCP are the centralized repository for all vulnerabilities and checklists

z/os System Checklists

The z System Checklist can be found at the NCP and/or directly from the DOD

Found at http://iase.disa.mil/stigs/

z/OS ACF2 STIGs

z/OS RACF STIGs

z/OS TSS STIGs

IBM Hardware Management Console (HMC) Stigs

z/os System Checklists

The current z/OS STIGs are version 6.14 and they do NOT just cover the operating system. The STIGs specify configuration controls, security controls and vulnerability controls.

The cover an entire range of IBM and Third Party Products and OS components.

The STIGS are updated on a quarterly basis. Version 6.14 was released on January 25th 2013

z/os System Checklists

The following is a list of products and components for the z/OS system that are covered by the DOD DISA STIGS:

- RACF
- ACF2
- TSS
- File Transfer Protocol
- z/OS UNIX SYSLOG
- TCP/IP Communications Server
- CA MIM

z/os System Checklists

- TN3270 Telnet Server
- z/OS UNIX Telnet Server
- Security Server (RACF) Settings
- CA Auditor
- Compuware Abend-AID
- CA-1 (Tape Management System)
- CA Common Services
- CICS Transaction Server

z/os System Checklists

- CL/Supersession
- Catalog Solutions
- BMC Control-D
- BMC Control-M
- BMC Control-O
- BMC Control-M/Restart
- Database Management Systems
- Fast Dump Restore

z/os System Checklists

- Front End Processor (FEP)
- Hardware Configuration Definition
- IBM Health Checker
- Integrated Cryptographic Service Facility
- Integrated Database Management System (IDMS)
- BMC IOA

z/os System Checklists

- SDSF
- Job Entry Subsystem 2 (JES2)
- BMC MainView
- NC-Pass Authenticator
- NetView
- Roscoe
- System Managed Storage (DFSMS)
- CSSMTP
- SRRAUDIT

z/os System Checklists

- Tivoli Asset Discovery for z/OS
- Transparent Data Migration Facility
- Time Sharing Option (TSO)
- UNIX System Services
- **Vanguard Security Solutions**
- CA Vtape
- VTAM
- WebSphere Application Server for z/OS
- WebSphere MQSeries for z/OS

Questions?