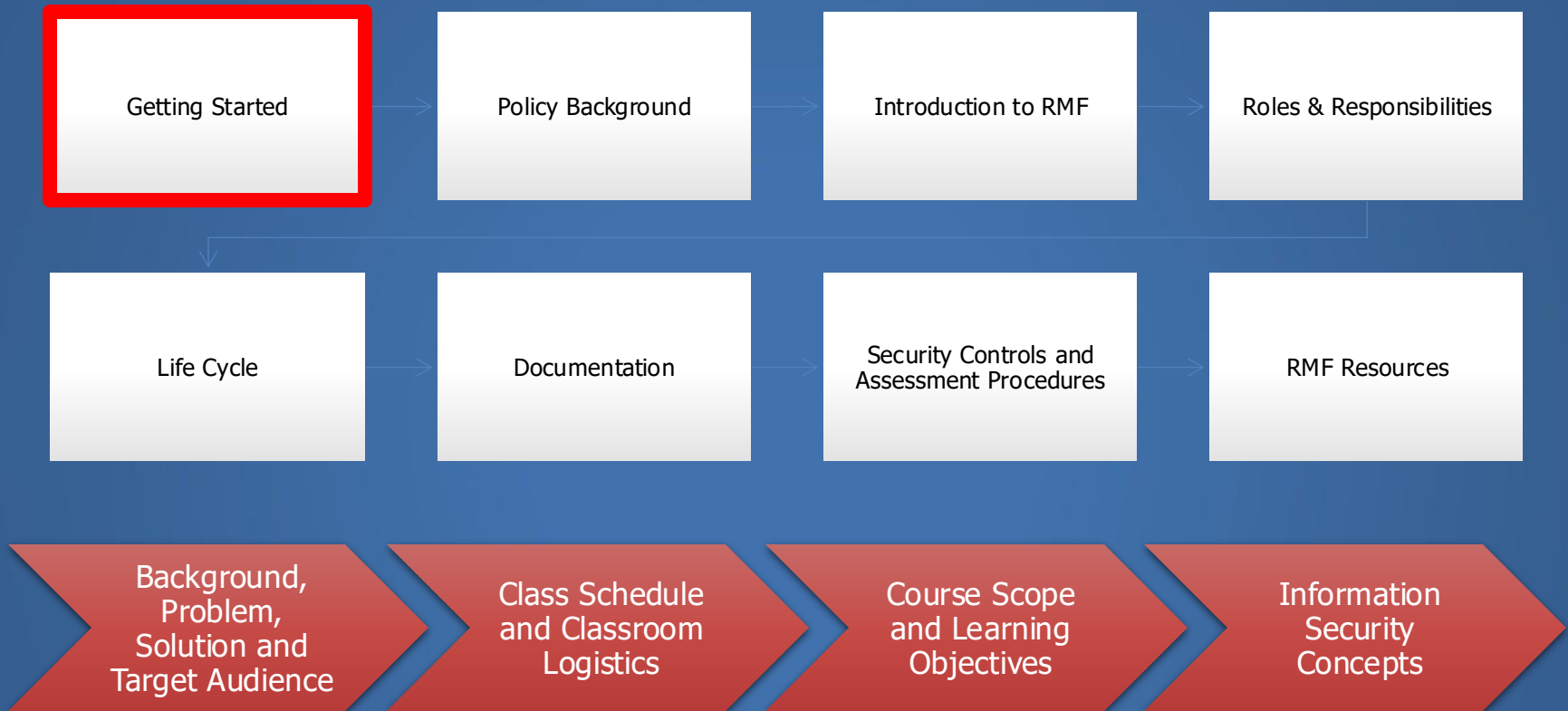




RISK MANAGEMENT FRAMEWORK (RMF) for Federal Agencies *Fundamentals* v7.0



BAI Background / Problem

- Risk Management Framework (RMF) is a life cycle process for managing information security risk
- RMF is now the standard risk management process for information systems in:
 - Federal Civilian departments/agencies
 - Intelligence community
 - DoD
- Employees and contractors from across the departments and agencies need to be educated in the RMF process
- This class will provide you with high-level knowledge of the Risk Management Framework (RMF)

BAI Target Audience

- This course has been developed for an audience who
 - Work or manage the area of information security
 - Work or manage in an IT environment (hardware, software, network, etc.)
 - Design, develop or maintain systems that require approval to operate in a Federal government environment

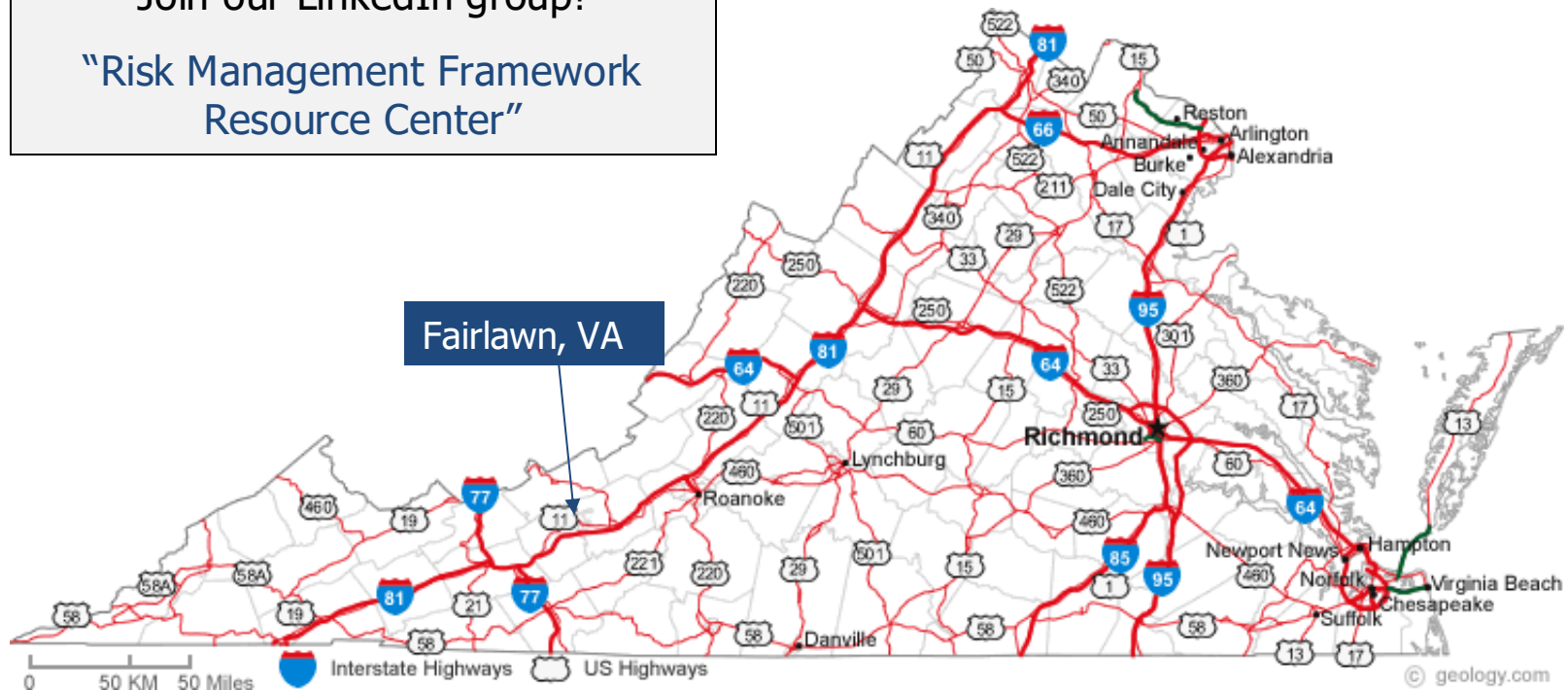
BAI Information Security Consulting and Training

"Risk Management Framework Resource Center"

<https://rmf.org>

Join our LinkedIn group!

"Risk Management Framework
Resource Center"



Meet Your Course Leader



BAI Participant Introductions

- Your name, affiliation and location?
- Are you a government or contractor employee?
- Your role?
- Your experience (if any) with RMF
- Something that others might not know about you



BAI This Class

- RMF for Federal Agencies Fundamentals is a one-day standalone course
- Also, first day of a four-day program:
RMF for Federal Agencies In Depth (three days) will follow
- Today's "estimated" time schedule
 - Morning: 3-3.5 hours (before lunch)
 - Lunch: 1 hour
 - Afternoon: 3 hours (after lunch)
 - Short breaks during morning & afternoon sessions
- Class format: Lecture and discussion

BAI Getting Started

■ Online Classroom



- Traditional Classroom
 - Building security, badges
 - Restrooms
 - Refreshments
 - Lunch suggestions
 - Internet access
- Course Materials:
 - Onsite students receive a hard-copy version of the slides
 - Online students receive a pdf file of today's class slides
- FA1-RMF for Federal Agencies Fundamentals



Questions are encouraged! Ask as they arise and/or during "Q&A".

BAI Course Scope

■ IN SCOPE

- Information security & risk management foundations
- RMF policy background
- Roles & responsibilities
- Life cycle steps
- Documentation
- NIST security controls and assessment overview
- Supporting resources

■ RMF IN DEPTH ONLY

- RMF life cycle steps guidance
- What goes into the documentation
- Detailed security controls
- Automated tools

■ OUT OF SCOPE

- Technical security engineering practices
- Program, system, or environment-specific guidance

BAI Learning Objectives

- This class has been designed to prepare you to be able to:
 - Describe fundamental concepts of information security and risk management
 - Describe relevant information security policies and guidance (e.g., FISMA, FIPS Publications, NIST Special Publications, CNSS Publications)
 - Identify the policy documents relating to RMF
 - Summarize the key RMF roles and responsibilities
 - Describe the major life cycle steps of the Risk Management Framework
 - Recall the key documents comprising the RMF “authorization package”
 - Explain the purpose and organization of the NIST Security Controls and Assessment Procedures
 - Identify primary online resources supporting the RMF process

BAI The Basics: Terminology

Information
Security

Information
Assurance

Cybersecurity

Same or different?

BAI The Basics: Formal Definitions

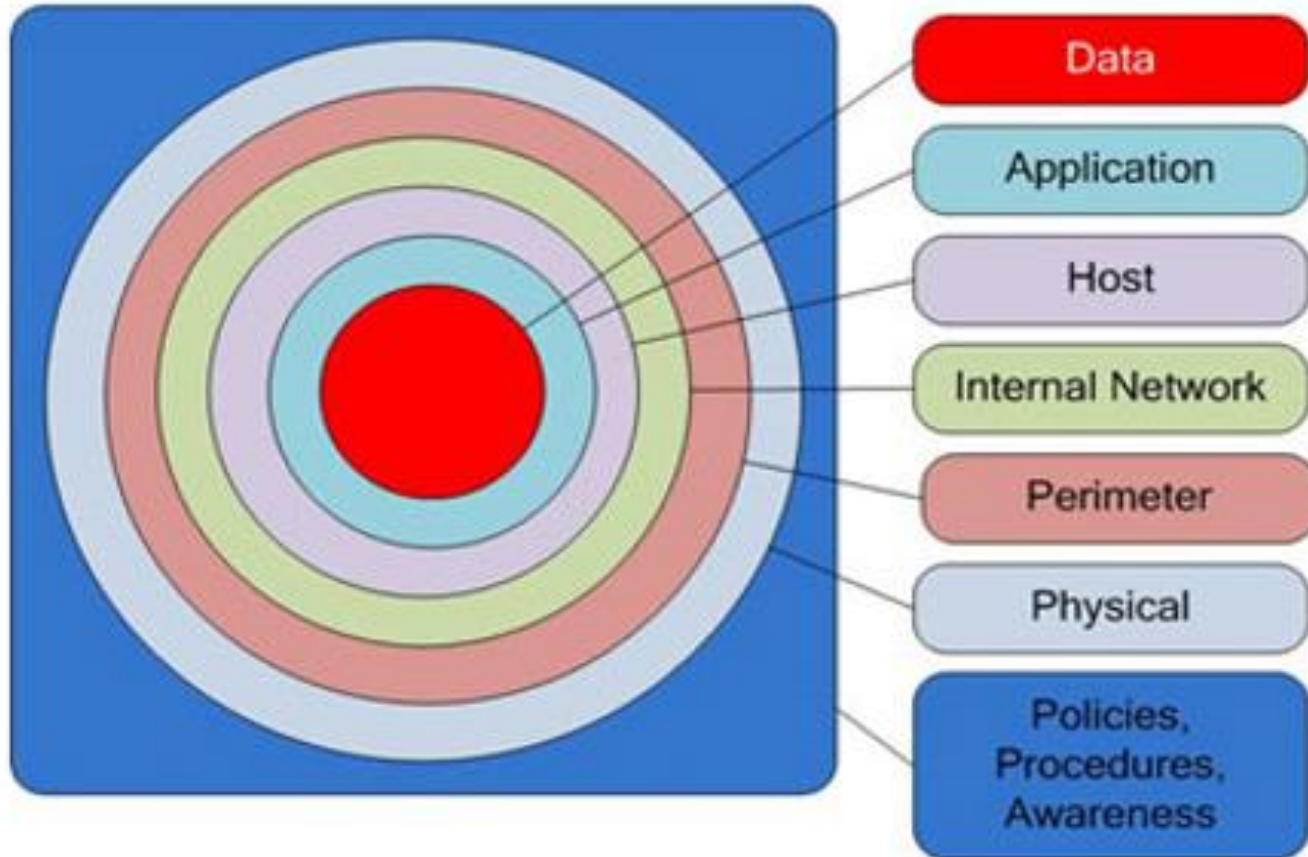
| Term | Definition* |
|-----------------------|---|
| Information Security | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. |
| Information Assurance | Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non- repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. |
| Cybersecurity | Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. |

* Source: CNSSI 4009, National Information Assurance Glossary, March 2022

BAI Information Security Concepts

- Effective information security:
 - People
 - Process
 - AND Tools
 - Goes beyond physical equipment and software that is processing the data
- Successfully protecting information means understanding multiple technical and non-technical security disciplines
- “Holistic view” of the information system

BAI Holistic View – Layers of Protection



Security Assessment and Authorization (CA)
Planning (PL)
Risk Assessment (RA)
System and Service Acquisition (SA)

MANAGEMENT

Awareness and Training (AT)
Configuration Management (CM)
Contingency Planning (CP)
Incident Response (IR)
Maintenance (MA)
Media Protection (MP)
Physical and Environmental Protection (PE)
Personnel Security (PS)
System and Information Integrity (SI)

OPERATIONAL

Access Control (AC)
Audit and Accountability (AU)
Identification and Authentication (IA)
System and Communications Protection (SC)

TECHNICAL



Personally Identifiable Information Processing and Transparency (PT)
Supply Chain Risk Management (SR)
Program Management (PM) (Driven by Tiers 1 & 2)

Source: NIST SP 800-53 R5

NIST SP 800-53 Rev 5 – Looking to the future!

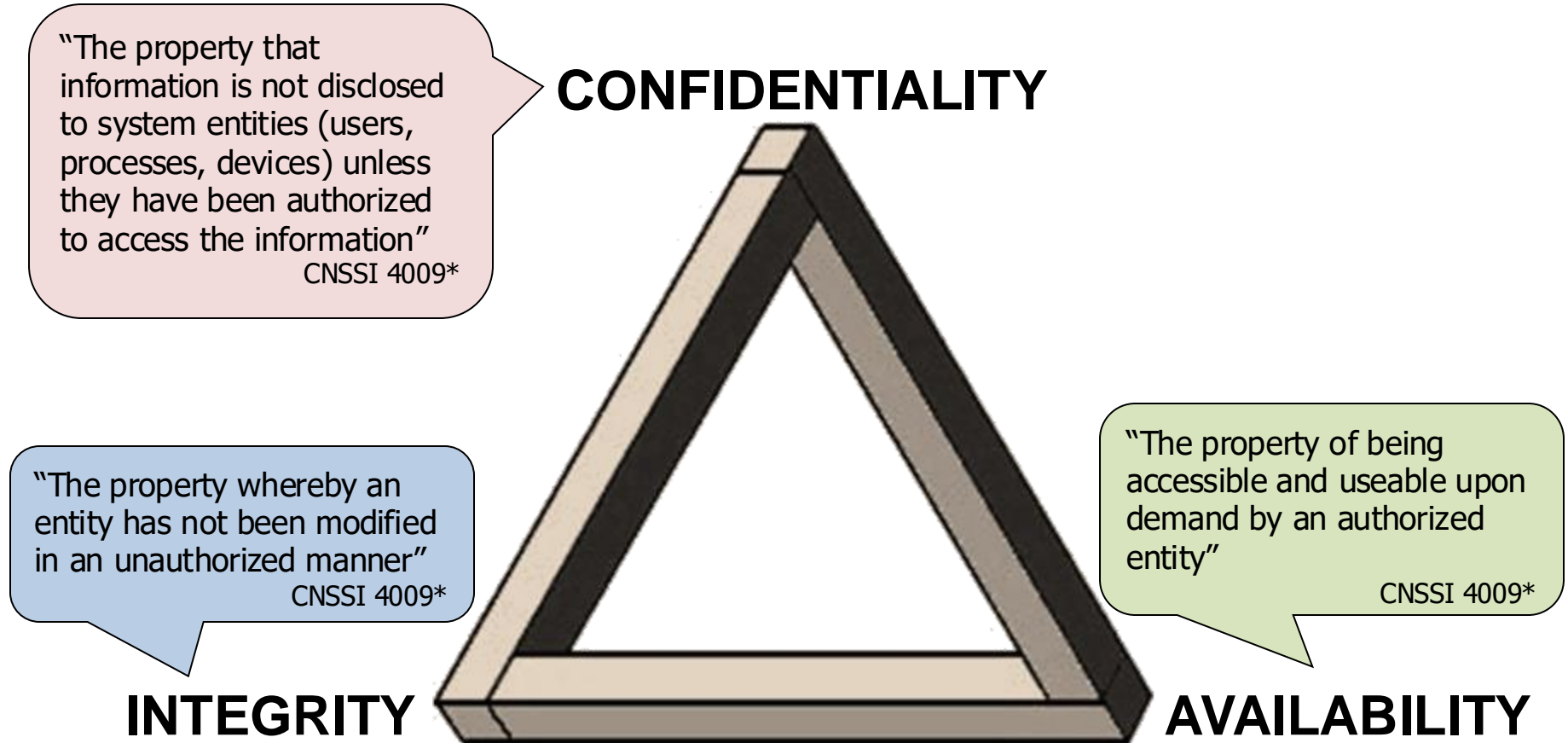
September 2020

| ID | FAMILY | ID | FAMILY |
|---------------------------|---|---------------------------|---------------------------------------|
| <u>AC</u> | Access Control | <u>PE</u> | Physical and Environmental Protection |
| <u>AT</u> | Awareness and Training | <u>PL</u> | Planning |
| <u>AU</u> | Audit and Accountability | <u>PM</u> | Program Management |
| <u>CA</u> | Assessment, Authorization, and Monitoring | <u>PS</u> | Personnel Security |
| <u>CM</u> | Configuration Management | <u>PT</u> | PII Processing and Transparency |
| <u>CP</u> | Contingency Planning | <u>RA</u> | Risk Assessment |
| <u>IA</u> | Identification and Authentication | <u>SA</u> | System and Services Acquisition |
| <u>IR</u> | Incident Response | <u>SC</u> | System and Communications Protection |
| <u>MA</u> | Maintenance | <u>SI</u> | System and Information Integrity |
| <u>MP</u> | Media Protection | <u>SR</u> | Supply Chain Risk Management |



Moves PM and Privacy Controls into the Main Body of Controls
 - Twenty Families – and adds a new family – Supply Chain Risk Management (SR)

Fundamental Principles of Information Security



*CNSSI 4009 – *National Information Assurance Glossary* (March 2022)

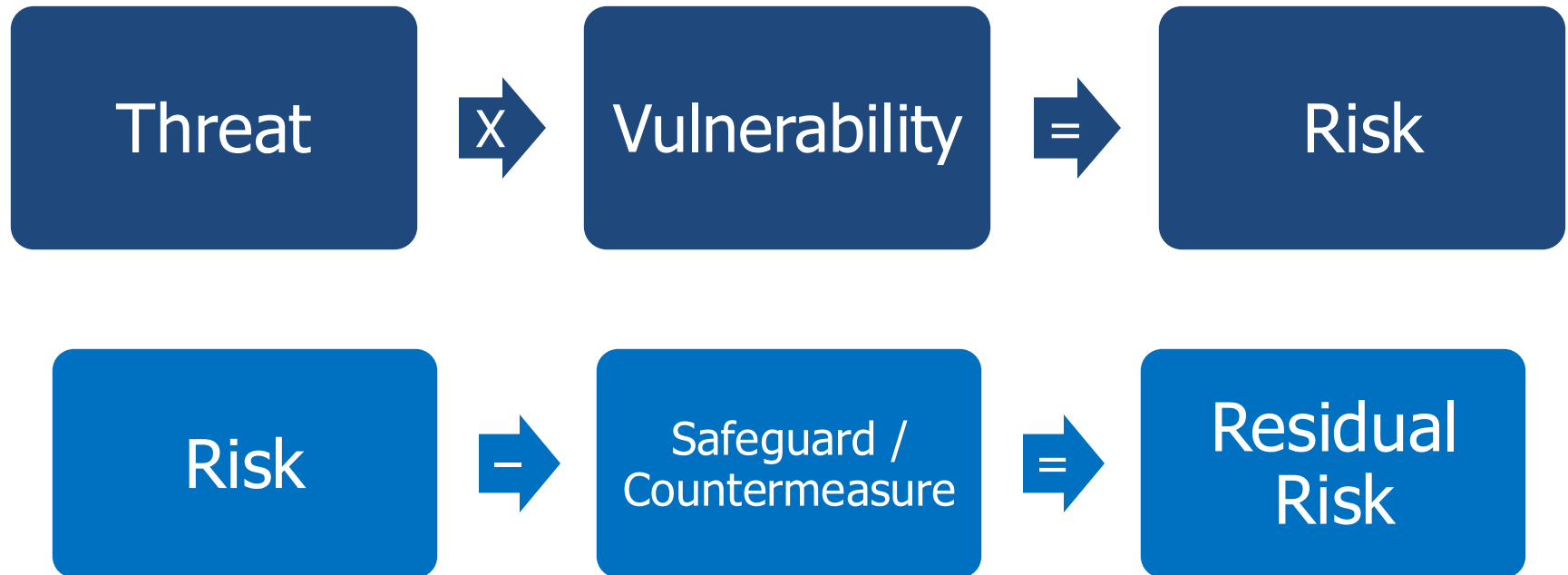
BAI Risk Management Model

Example threats:

1. Natural (snowstorms, floods, tornadoes)
2. Terminated employee accessing proprietary information.
3. Theft, vandalism, fire
4. Unauthorized access to information based on known software vulnerabilities.

Example vulnerabilities:

1. Geographic location
2. Lack of due diligence to protect property and assets
1. Defect in software code exploited when patching is not current



BAI Quantifying Risk

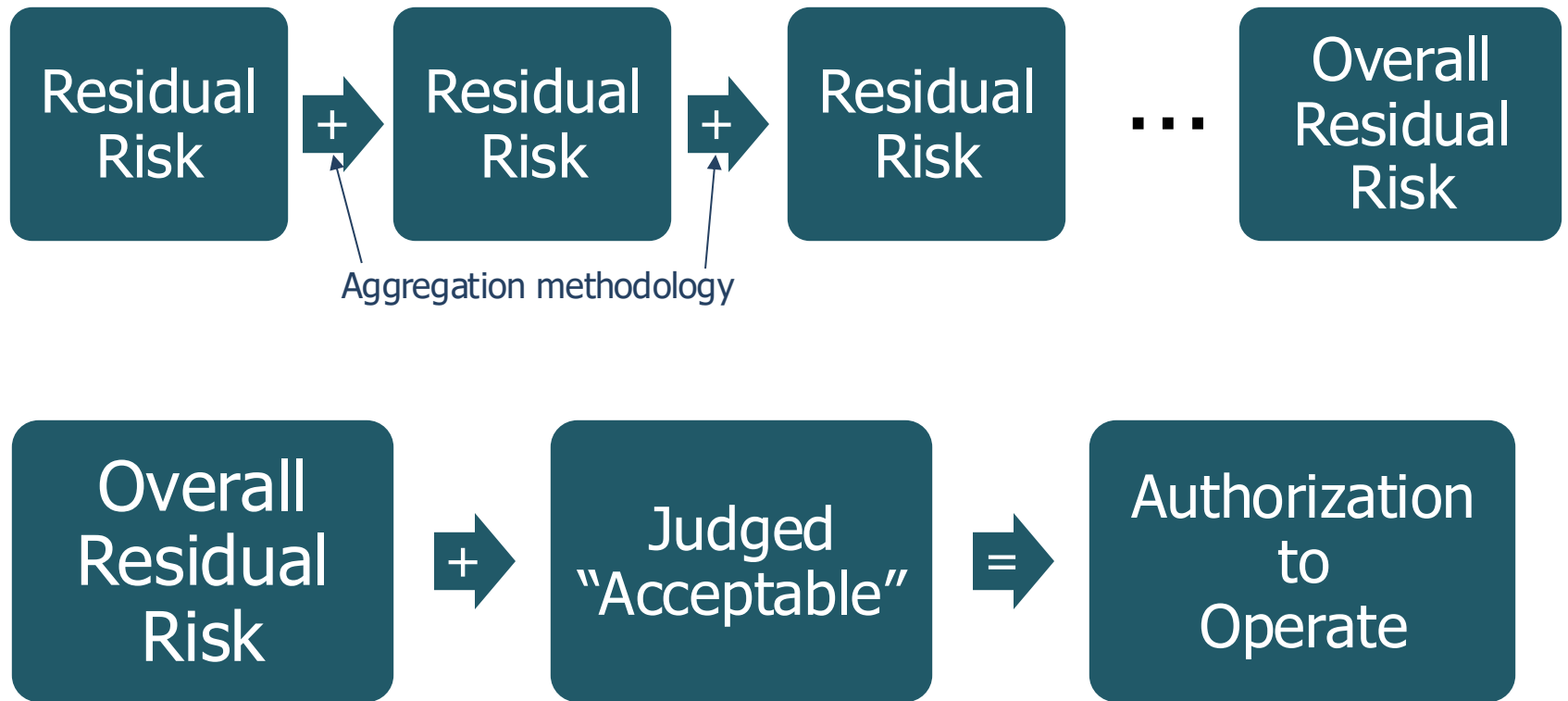
Example Impact: Monetary loss, loss of reputation, loss of competitive advantage



| Likelihood (Threat Event Occurs and Results in Adverse Impact) | Level of Impact | | | | |
|---|-----------------|----------|----------|----------|-----------|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

Source: NIST Special Publication 800-30

BAI Acceptance of Risk



BAI Who Accepts the Risk?

- The Authorizing Official (AO):
 - A senior government employee
 - Determines if residual risk is acceptable
 - Before a system is permitted to be placed into operation

What word would you use to describe the type of decision the AO makes in saying the residual risk is/is not acceptable?

BAI Note to Contractors

- Contractors must build and maintain systems in accordance with government standards
- However, the government is ultimately responsible for accepting the risk and authorizing the system for operation
- Now NIST SP 800-171 (Cybersecurity Maturity Model Certification - CMMC) will place specific security requirements on Contractors

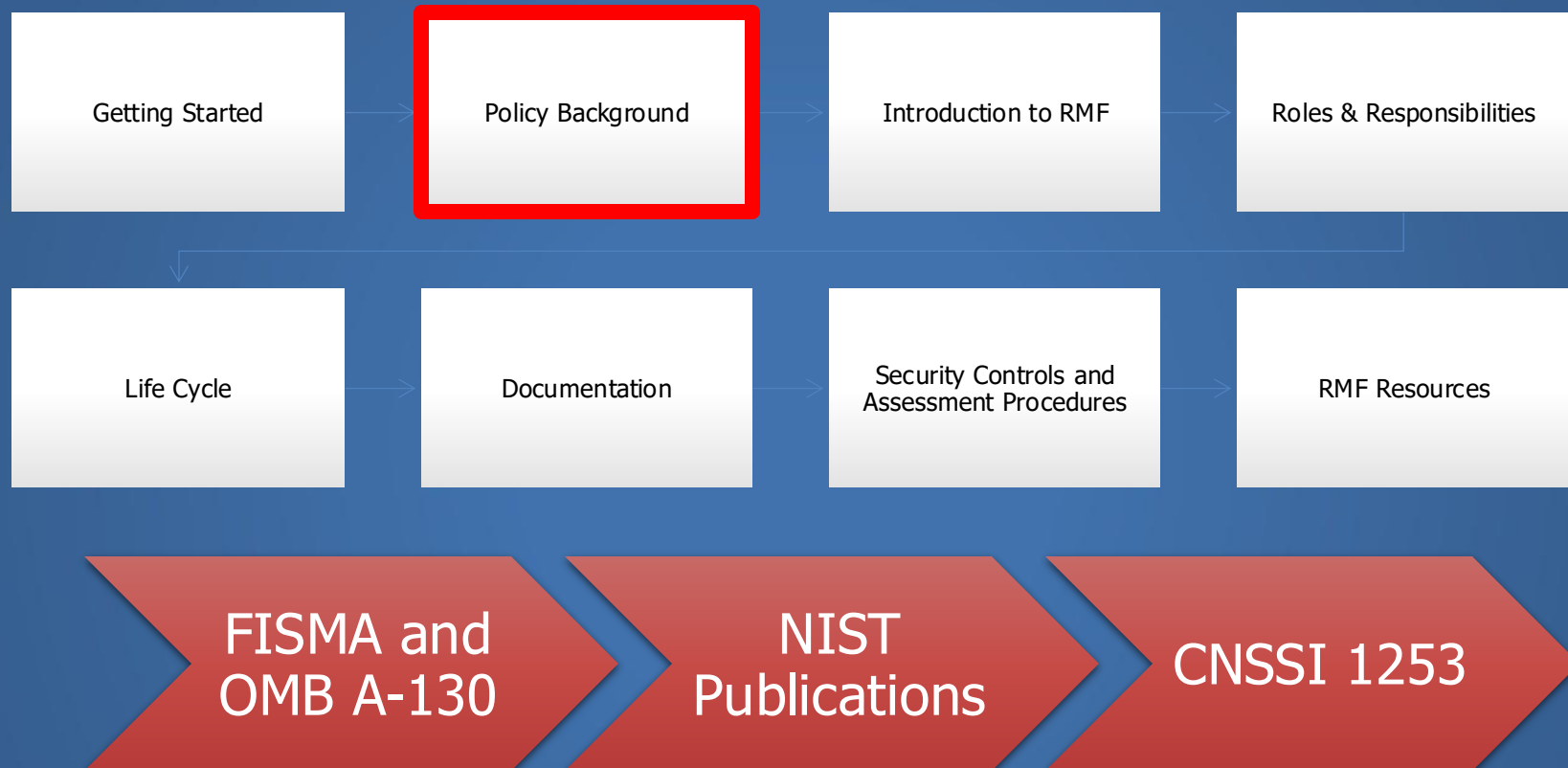
BAI Pop Quiz

- What are the three fundamental information security objectives?
- What is “residual risk”?
- What two factors are used to quantify the level of risk?
- What is “acceptable risk”?
- Who is responsible for “accepting” risk and authorizing operation?

TRUE OR FALSE? The mission of the information security program in any organization is to effectively manage risk.



- The perception of information security as an “overarching” activity is conducive to success
- Information security objectives are to protect information and systems:
 - Confidentiality
 - integrity, and
 - availability
- Information security encompasses both technical and non-technical areas (“holistic view”) and provides layers of protection.
- Risk is a combination of threats and vulnerabilities; safeguards are implemented to reduce (mitigate) risk
- Level of residual risk must be deemed acceptable by the government before a system is authorized for operation





- Title III, E-Government Act of 2002 (PL 107-347)
- Federal Information Security Management Act (FISMA) applies to all organizations that:
 - Use or possess Federal information
 - Operate, use or access Federal information systems
- Applies to Executive Branch* organizations
 - Federal Civilian departments/agencies
 - DoD
 - Intelligence Community
- State/local governments that process federal data or use federal information systems
- Contractors and industry partners that process federal data or use federal information systems

*Does not apply to
Legislative (Congress) or
Federal Judiciary (Court)
system.

BAI FISMA Highlights

- Each agency to develop, document and implement an agency-wide information security program, including:
 - Policies and procedures
 - Security awareness training
 - Periodic risk assessments
 - Testing and evaluation of security controls at least annually
 - Process to address security deficiencies
 - Incident response procedures
 - Continuity of operations plans/procedures
 - Annual review of information security program, with results reported to the Office of Management and Budget (OMB)
- OMB to prepare an annual report to Congress on agency compliance with FISMA
- National Institute of Standards and Technology (NIST) to develop IT security guidelines

- The Federal Information Security Modernization Act (FISMA) 2014 updates the federal governments cybersecurity practices:
 - **Authorizes DHS to provide operational and technical assistance** to other federal Executive Branch civilian agencies at the agency's request;
 - **Places the federal information security incident center** (a function fulfilled by [US-CERT](#)) **within DHS** by law;
 - **Authorizes DHS technology deployments to other agencies' networks** (upon those agencies' request);
 - **Directs OMB to revise policies regarding notification of individuals** affected by federal agency data breaches;
 - **Requires agencies to report major information security incidents as well as data breaches to Congress as they occur** and annually; and
 - **Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting** while adding new reporting requirements for major information security incidents. **Resulted in update of OMB A-130 circular.**

OMB Circular A-130 – basis of “traditional” federal IS Certification & Accreditation

- Published 1985/updated 2000 (Appendix III)
 - Roles & Responsibilities
 - Information system types
 - System Security Plan
 - Security Controls Assessment
 - Re-authorization at least once every three years

- Updated 2016 – Cyber Security Focus (Appendix I)
 - Categorize information systems
 - Establish agency-wide risk management process
 - Implement security controls per NIST guidance
 - Develop Security Plans to document security controls
 - Implement continuous monitoring strategy
 - Implement ongoing reauthorization (replace 3-yr authorization)

- FISMA specifically tasked NIST to develop IT security guidance
- FISMA Implementation Project:
<http://csrc.nist.gov/groups/SMA/fisma/>
- NIST Publications
 - Mandatory: Federal Information Processing Standard (FIPS) Publications
 - FIPS 140-2 – Security Requirements for Cryptographic Modules
 - FIPS 201-2 – Personal Identity Verification (PIV)
 - Guidance: NIST Special Publications (NIST SP)
 - NIST SP 800-34 – Contingency Planning Guide
 - NIST SP 800-153 – Guide to Securing Wireless Local Area Networks (WLANs)
 - Covers a wide variety of subject areas, both technical and non-technical

BAI Key RMF Related NIST Pubs

| Publication | Full Title |
|------------------------------------|--|
| FIPS 199 | Standards for Security Categorization of Federal Information and Information Systems |
| FIPS 200 | Minimum Security Requirements for Federal Information and Information Systems |
| NIST SP 800-30 Rev 1 | Guide for Conducting Risk Assessments |
| NIST SP 800-37 Rev 2 | Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy |
| NIST SP 800-39 | Managing Information Security Risk: Organization, Mission, and Information System View |
| NIST SP 800-53 Rev 4 and Rev 5 | Security and Privacy Controls for Information Systems and Organizations |
| NIST SP 800-53A Rev 4 and Rev 5 | Assessing Security and Privacy Controls in Information Systems and Organizations |
| NIST SP 800-60 | Guide for Mapping Types of Information and Information Systems to Security categories |
| NIST SP 800-137 | Information Security Continuous Monitoring for Federal Information Systems and Organizations |
| NIST SP 800-137A | Assessing Information Security Continuous Monitoring (ISCM) Programs |

BAI NIST SP 800-37 R2 (RMF 2.0)

- “Risk Management Framework for Information Systems and Organizations, A System Lifecycle Approach for Security and Privacy”
- Key NIST document in the application of RMF to federal systems
- Published December 2018
- Several significant changes to develop the next-generation Risk Management Framework (RMF) for information systems, organizations, and individuals.

BAI SP 800-37 Rev2

Formally Adopts a "Prepare" Step

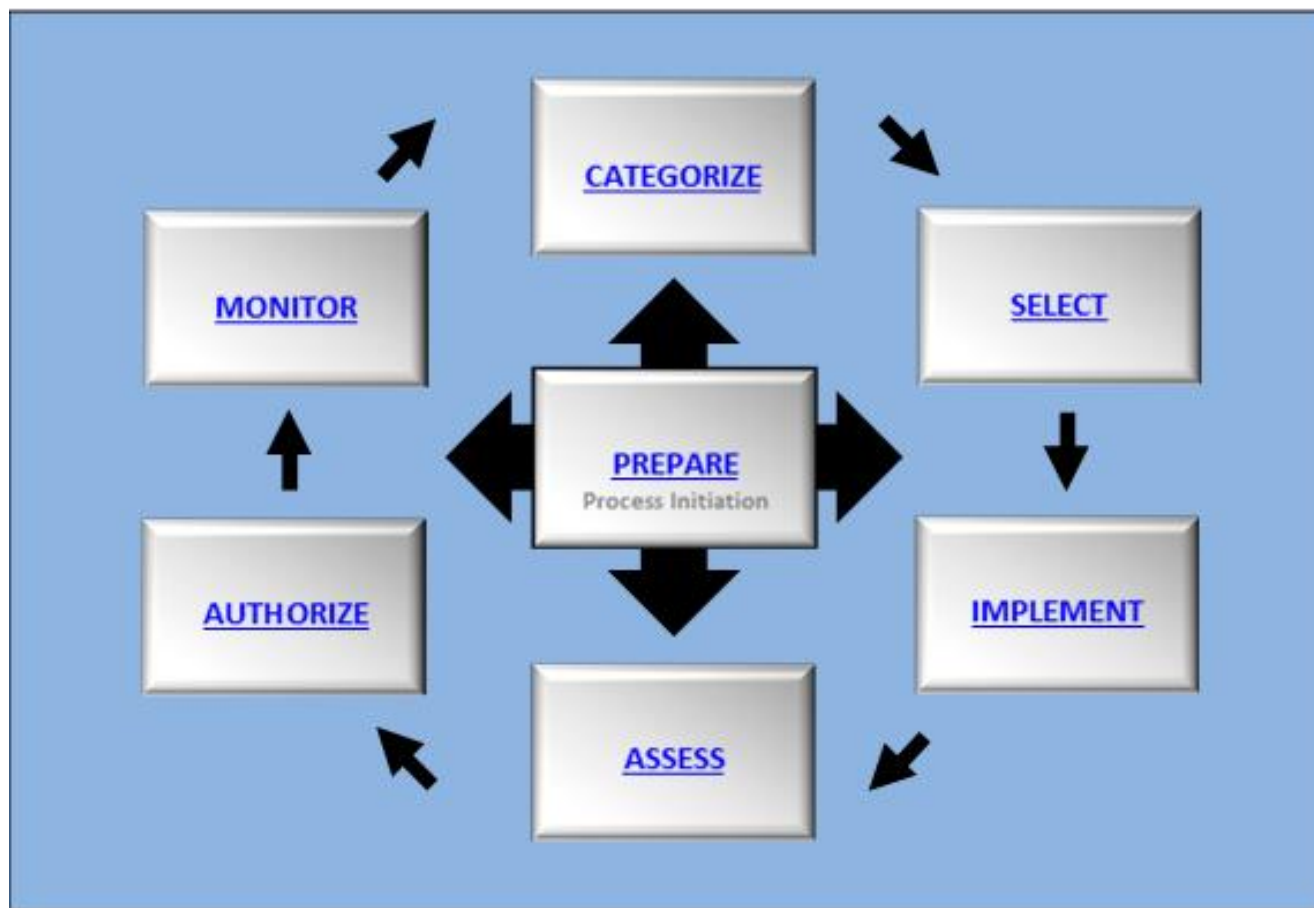


FIGURE 2: RISK MANAGEMENT FRAMEWORK

- Significant changes:
 - To provide organizational-tailored baselines and common enterprise controls to reduce work at the system level – part of a new step called “Preparation”
 - To provide a closer link between the RMF process and the governance of the organization
 - To ensure organization-wide risk management strategy to facilitate a more efficient and cost-effective execution of RMF
 - To align the Cybersecurity Framework with RMF processes
 - To integrate privacy risk management concepts into RMF
 - To promote development of trustworthy secure software and systems utilizing systems engineering processes in NIST SP 800-160
 - To integrate supply chain risk management concepts (SCRM) into RMF

Committee on National Security Systems (CNSS)

Instructions 1253 & 1254 for NSS



- CNSS:
 - Interagency committee with a presidential mandate (NSD-42) to protect National Security Systems and communications
 - Publish numerous policies, directives, instructions, etc.
 - CNSSI 1253, "Security Categorization and Control Selection for National Security Systems", is the one directly relevant to RMF
 - CNSSI 1254, "Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems"
 - Defines core documents required in the Authorization package
 - Contains data elements in the RMF core authorization documents
 - Provides information on the reciprocity process for NSS

BAI What is a National Security System?

- National Security Systems (NSS) are information systems operated by US Government, its contractors, or agents, that contain classified information or that:
 - involve intelligence activities
 - involve cryptographic activities related to national security
 - involve command and control of military forces
 - involve equipment that is an integral part of a weapon or weapons system(s);
 - are critical to the direct fulfillment of military or intelligence missions (not including routine administrative and business applications); or
 - is always protected by procedures established for information that have been specifically authorized under criteria established by an executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy (44 U.S.C. § 3552)

Resource: NIST SP 800-59, Guidelines for Identifying an Information System as a National Security System

- The Risk Management Framework relies on publications from several government entities
- FISMA is the overarching legislation
- OMB Circular A-130 introduced the concept of system authorization and updated in August 2016
- NIST publishes a large library of RMF guidance documents (Special Publications) for adoption/adaptation by agencies, as well as a smaller number of FIPS Publications, which are mandatory
- CNSSI 1253 is applicable to all National Security Systems (including Federal Civilian agencies)

BAI RMF “Publications Library”



Copies of the RMF publications we discuss in this class are available on the BAI RMF Resource Center website.

<https://rmf.org/rmf-documents>

Consider downloading these publications to your Kindle or computer tablet for some “light reading on the go”.

Introduction to RMF

Getting Started

Policy Background

Introduction to RMF

Roles & Responsibilities

Life Cycle

Documentation

Security Controls and
Assessment Procedures

RMF Resources

What is RMF?

Where did it
come from and
why is it better?

How RMF relates
to the System
Development Life
Cycle

How RMF relates
to the federal
acquisition
process

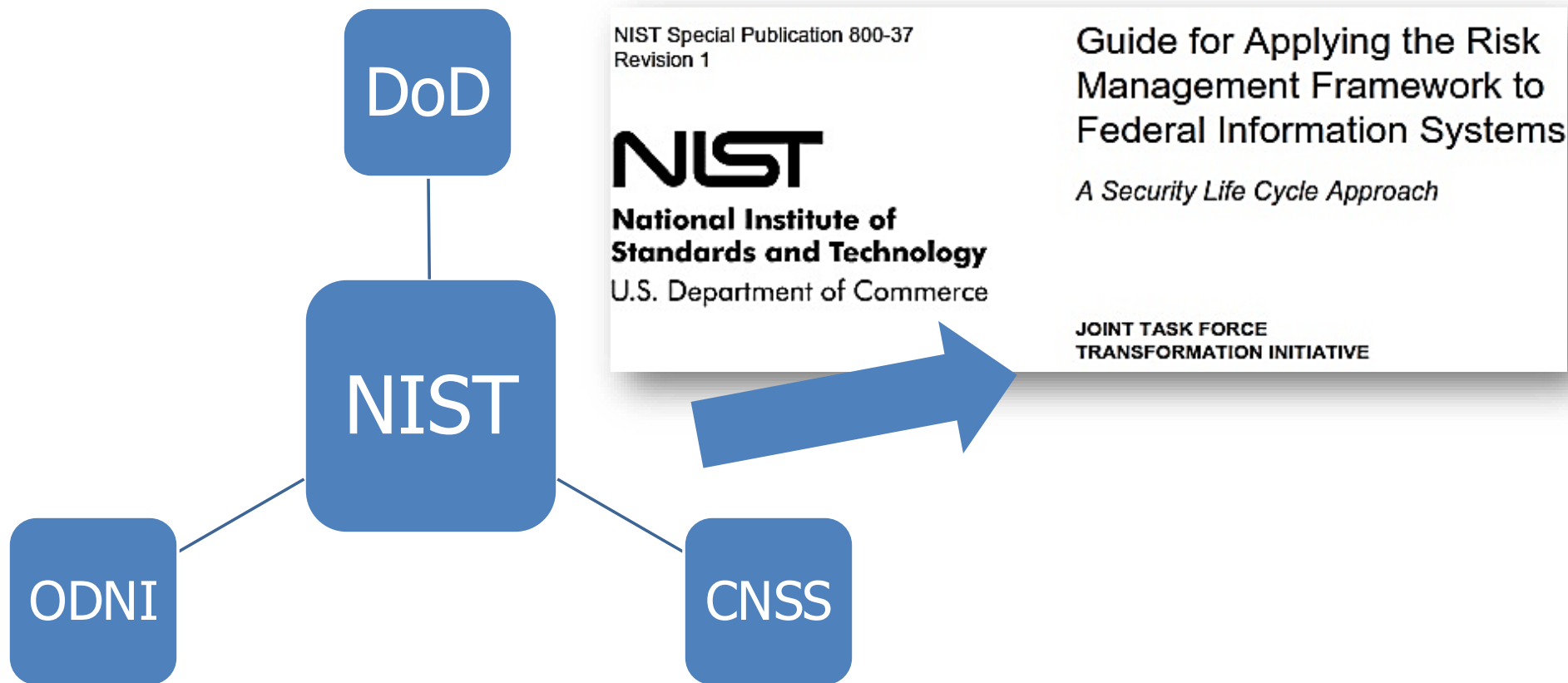
RMF "building
blocks"

BAI What is the Risk Management Framework (RMF)?

- RMF is the “common information security framework for the federal government and its contractors”
- RMF goals
 - Improve information security
 - Strengthen risk management processes
 - Encourage reciprocity among federal agencies

BAI Who Is the Developer of RMF?

Joint Task Force Transformation Initiative Working Group



BAI What Makes RMF "Better"?

- Emphasis on continuous monitoring to enable near real-time risk management and ongoing system authorization
- Encouraging the use of automation to provide timely information to leadership so they can make risk-based decisions
- Integration of information security into enterprise architecture and the system development life cycle
- Emphasis on selection, implementation, assessment and monitoring of security controls, and authorization of information systems
- Linking risk management at the information system level to risk management at the organizational level through the risk executive (function)
- Establishing accountability for security controls that can be inherited

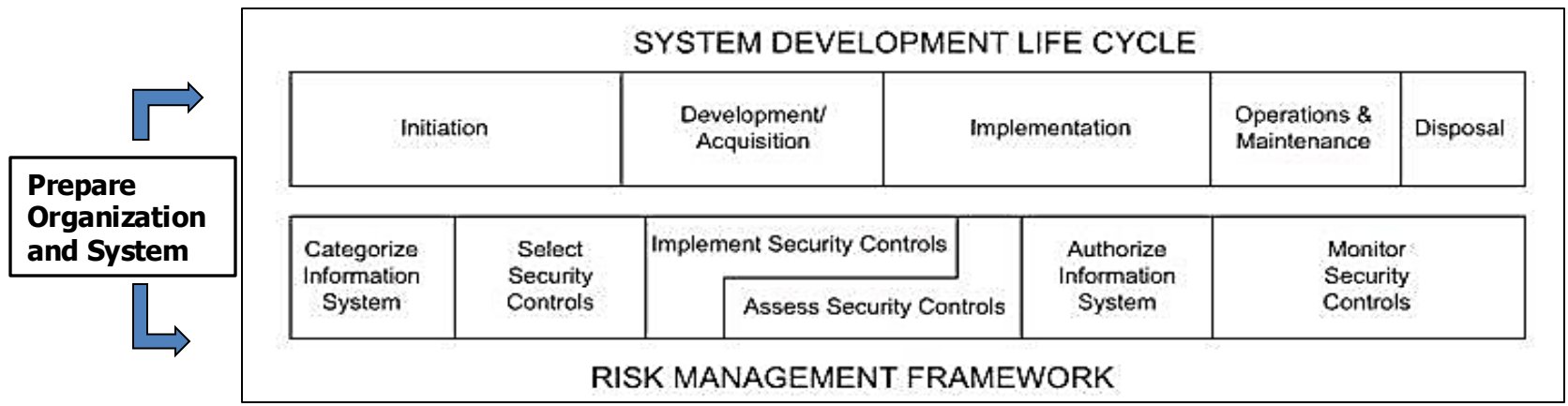
RMF represents a shift from traditional Certification and Accreditation (C&A) to a "more dynamic approach"

BAI System Development Life Cycle

- The system development life cycle is the overall process of developing, implementing, and retiring information systems through a multistep process
- 5 Phases of the SDLC:
 - Initiation
 - Development/Acquisition
 - Implementation
 - Operations/Maintenance
 - Disposal

RMF and System Development Life Cycle (SDLC)

- RMF is intended to integrate with all phases of SDLC, for example, by introducing security requirements in the Initiation phase
- Each of the RMF Life Cycle steps and tasks can be correlated to the appropriate SDLC phase(s)



Control Implementation

Task I-1: Implement the controls in the security and privacy plans.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Information Owner or Steward; Security Architect; Privacy Architect; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer; Enterprise Architect; System Administrator.

System Development Life Cycle Phase: **New** - Development/Acquisition; Implementation; **Existing** – Operations/Maintenance

RMF and Federal Acquisitions - Federal Acquisition Regulation (FAR)

- "The agency head or a designee shall prescribe procedures for ensuring that agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544), OMB's implementing policies including Appendix I of OMB Circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology."

BAI RMF “Building Blocks”

- Roles and Responsibilities
- Life Cycle Steps
- Documentation
- Security Controls and Assessment Procedures

Each of these “building blocks” will be covered in a separate unit of this class

- RMF is the “unified framework” for federal information security
- RMF was developed by the Joint Task Force Transformation Initiative (which includes NIST, DoD, the intelligence community, and CNSS)
- RMF was designed to integrate with the System Development Life Cycle
- The Federal Acquisition Regulation (FAR) requires RMF be integrated into the acquisition process
- The “building blocks” of RMF are
 - Roles and responsibilities
 - Life cycle
 - Documentation
 - Security controls and assessment procedures

Roles and Responsibilities

Getting Started

Policy Background

Introduction to RMF

Roles & Responsibilities

Life Cycle

Documentation

Security Controls and
Assessment Procedures

RMF Resources

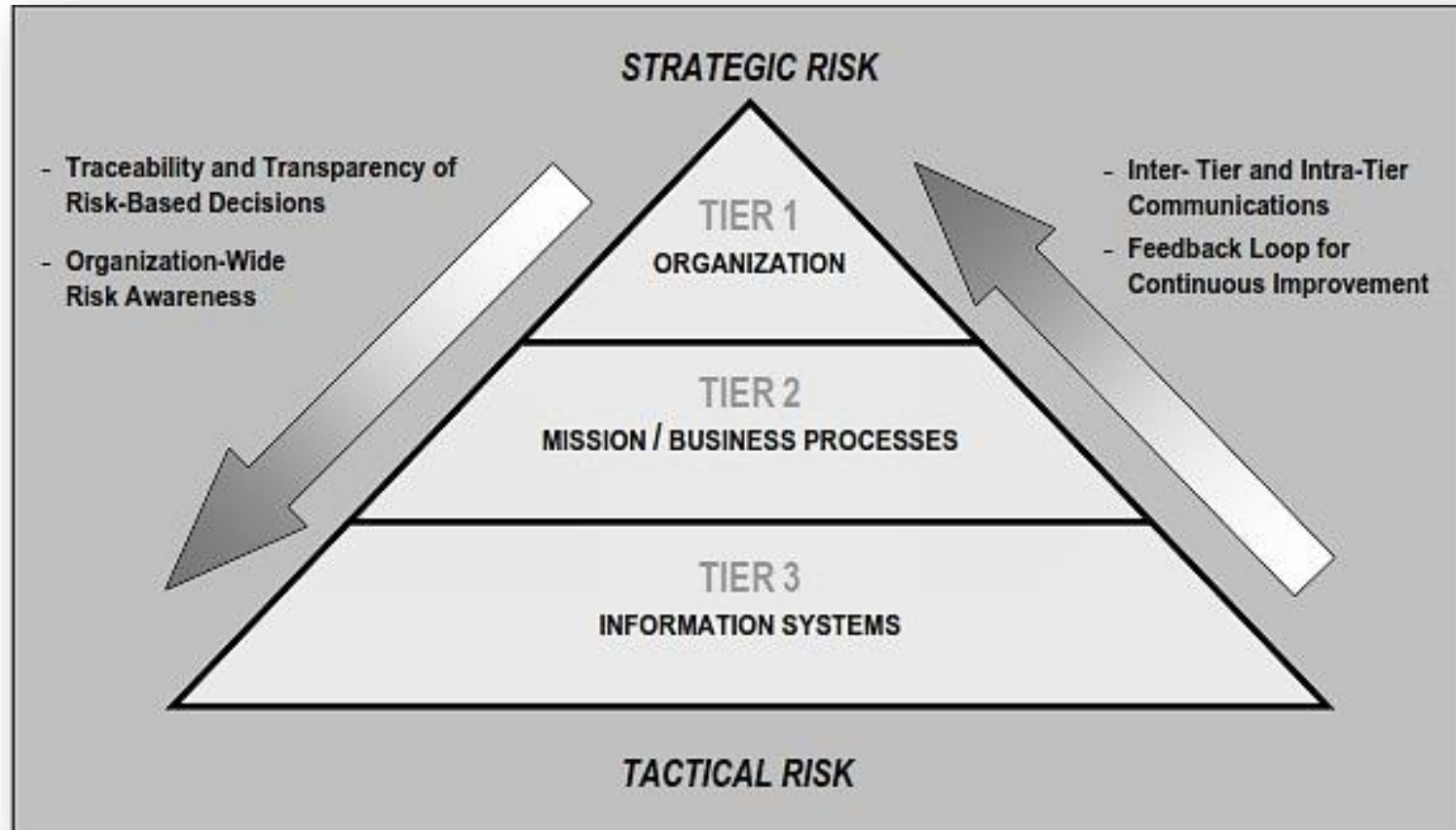
NIST three-tier
model of risk
management

Tier 1
(organization)
roles

Tier 2
(mission/business
process) roles

Tier 3
(information
system) roles

BAI Three-tier Model of Risk Management (NIST)



Source:

NIST SP 800-39, *Managing Information Security Risk – Organization, Mission and Information System View*, March 2011

BAI Top-level RMF Roles (NIST)

Source
NIST SP 800-37 R2



* These roles are assigned to government employees only



Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA)



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**

COVID Questions

Report Cyber Issue

- CYBERSECURITY
- INFRASTRUCTURE SECURITY
- EMERGENCY COMMUNICATIONS
- NATIONAL RISK MANAGEMENT
- ABOUT CISA
- MEDIA

Cybersecurity > Securing Federal Networks

Cybersecurity

- Cybersecurity Training & Exercises
- Cybersecurity Summit 2020
- Cyber QSMO Marketplace
- Combating Cyber Crime
- Securing Federal Networks ▾**
- Protecting Critical Infrastructure
- Cyber Incident Response
- Cyber Safety
- Cybersecurity Assessments
- Cybersecurity Governance
- Cybersecurity Insurance
- Detection and Prevention

SECURING FEDERAL NETWORKS

The federal enterprise depends on information technology (IT) systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems.

The Cybersecurity and Infrastructure Security Agency (CISA) works with each federal civilian department and agency to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats. As systems are protected, alerts can be issued at machine speed when events are detected to help protect networks across the government information technology enterprise and the private sector. This enterprise approach will help transform the way federal civilian agencies manage cyber networks through strategically sourced tools and services that enhance the speed and cost effectiveness of federal cybersecurity procurements and allow consistent application of best practices.

[Expand All Sections](#)

Capacity Enhancement Guides

National Cybersecurity Protection System (NCPS)

Continuous Diagnostics and Mitigation (CDM)

Securing Federal Networks

- CDM
- EINSTEIN
- Federal Information Security Management Act
- HVA PMO
- National Cybersecurity Protection System
- Network Security Deployment
- Quality Services Management Office
- Risk Management Framework Assessment and Authorization Service Offerings
- Security and Awareness Training
- Situational Awareness and Incident Response
- Trusted Internet Connections

<https://www.cisa.gov/securing-federal-networks>

BAI System-level (Tier 3) Roles

- Authorizing Official (AO)
- Authorizing Official (AO) Designated Representative
- Information System (IS) Cybersecurity Program
 - Information System Owner (ISO)
 - Names vary and may include Program Manager / System Manager (PM/SM) as well as others
 - Information System Security Officer (ISSO)
 - Some agencies may include an Information System Security Manager (ISSM) to handle management related tasks

BAI Authorizing Official (AO)

- Has authority to formally accept risk on behalf of the organization
- Senior-level government employee with budgetary oversight for a system or are responsible for business and/or mission process(es) supported by the system
- Responsibilities:
 - Make authorization decisions for Information Systems within their purview
 - Ensure RMF tasks are completed and documented
 - Approve SSPs, MOAs/MOUs, etc.
 - Track POA&Ms
 - Determine whether significant changes to an IS require reauthorization
- Authorization decisions cannot be delegated; all other responsibilities can be delegated to AO Designated Representative (AODR)

Authorizing Official (AO) Designated Representative

- Acts on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated with the security authorization process
- Make certain decisions regarding the planning and resourcing of the security authorization process
- Can approve the security plan
- Approve and monitor the implementation of plans of action and milestones, and the assessment and/or determination of risk
- CAN prepare the final authorization package, obtain the AO's signature on the authorization decision document, and transmit the package to appropriate organizational officials
- CANNOT make the authorization decision
- CANNOT sign the authorization decision document

BAI Information System Owner (ISO) [1 of 2]

- Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system
- Plans and budgets for security control implementation, assessment and sustainment
- Categorizes assigned systems (in conjunction with the Information Owners)
- Addresses the operational interests of the user community
- Ensures users and support personnel receive cybersecurity training (i.e., initial and ongoing, rules of behavior, role-based, etc.)
- Develops a system description (including boundary)
- Enforces AO authorization decision
- Responsible for ensuring compliance with information security requirements

BAI Information System Owner (ISO) [2 of 2]

- Serves as the focal point of the information system, both as an owner and as the central point of contact between the authorization process and system component owners
 - Applications, networking, servers, or workstations
 - Owners/stewards of information
 - Owners of the missions and business functions supported
- With the Information System Security Officer (ISSO)
 - Develops and maintains the security plan
 - Ensures the system is deployed and operated in accordance with the agreed-upon security controls
- With the information owner/steward
 - Decides who has access to the system, as well as types of privileges and access rights
 - Ensures system users and support personnel receive the requisite security training
- May also be referred to as Program Manager or Business/Asset Owner

BAI Information System Security Officer (ISSO)

- Ensure information owners / stewards are identified
- Maintains a repository for cybersecurity documentation for systems
- Ensure cybersecurity documentation is up-to-date and accessible to authorized individuals
- Respond to cybersecurity incidents
- Enforce cybersecurity policies and procedures
- *Collaborates* with system owner to ensure appropriate operational security posture is maintained for an information system
- Serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system
- May assist in developing security policies and procedures
- Ensures compliance with security policies and procedures
- Assigned management responsibility for day-to-day security operations of a system and its environment

NOTE: Organizations may also define an *information system security manager* or *information security manager* role with similar responsibilities as an information system security officer or with oversight responsibilities for an information security program.

BAI Additional Roles

- Information Owner / Steward (IO)
- Common Control Provider
- Information System Security Engineer
- Information Security Architect
- Contracting Officer or Agent

NOTE: These are most often Tier 3 roles, but in some cases, they can exist in Tiers 1 and/or 2.

BAI Information Owner/Steward (IO)

- Official with statutory, management or operational authority for specified information
- Responsible for establishing policies and procedures for generation, collection, processing, dissemination and disposal of the information
- May or may not be the Information System Owner
- A single system may contain information from multiple IOs
- In information-sharing environments, responsible for establishing the rules for appropriate use and protection of the information
 - Retains that responsibility when information is shared with – or provided to – other organizations
- Provides input to information system owners regarding the security requirements and security controls for the systems where the information is processed

BAI Common Control Provider

- An individual, group or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems)
- Typically, not assigned as a separate, discrete, role but rather in conjunction with responsibility related to implementation and maintenance of a security control or control family
- Documents the organization-identified common controls in a security plan (or equivalent)
- Ensures assessments of common controls are carried out by qualified assessors with a level of independence as defined by the organization
- Produces Plan of Action and Milestones (POA&Ms) for common controls

Information Security Architect (ISA)



Information System Security Engineer (ISSE)

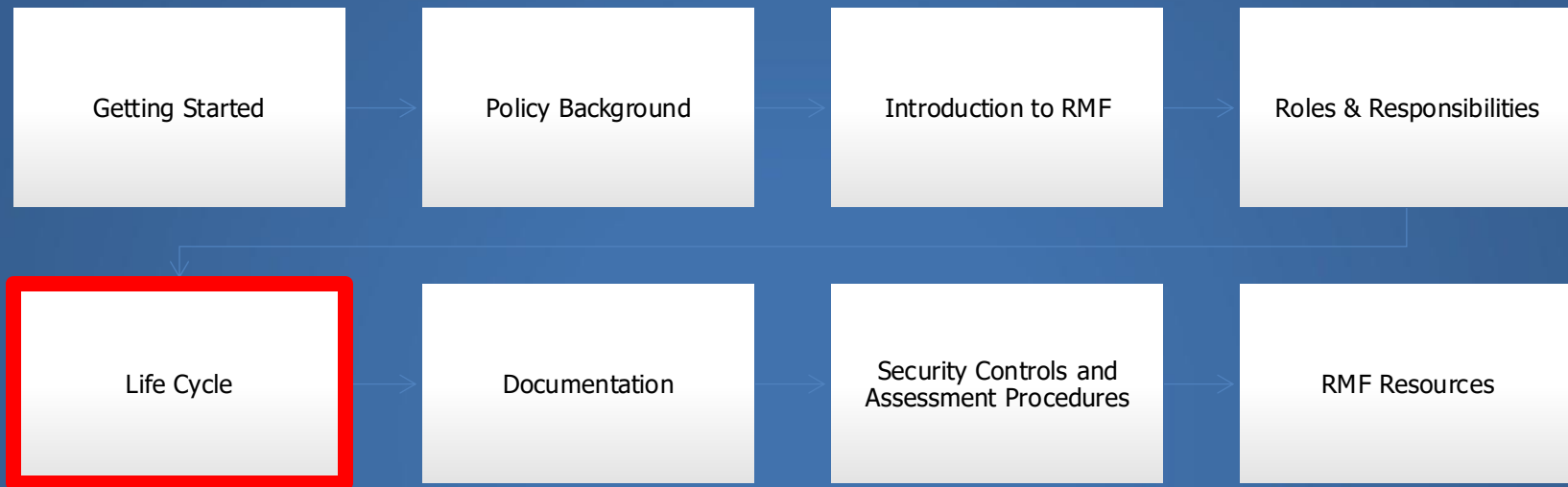
Information Security Architect (ISA)

- Ensures security requirements are integrated into enterprise architecture
- Liaison between the Enterprise Architect (EA) and the ISSE
- Helps define and allocate controls as system-specific, hybrid, or common
- Advises decision makers on a variety of security-related issues

Information System Security Engineer (ISSE)

- Ensures security requirements are integrated into information system and product acquisition, design and configuration
- An integral part of a system development team
- Captures, refines and integrates security requirements into system designs

- NIST defines a three-tier model for risk management
 - Tier 1 – Organization
 - Tier 2 – Mission/Business Process
 - Tier 3 – Information Systems
- Tier 1 and 2 roles include Agency Head, CIO, SISO, Risk Executive (function)
- Tier 3 roles include AO, ISO, PM/SM, ISSO/ISSM
- Additional roles include IO, Common Control Provider, ISA, ISSE



Types of IT Systems

RMF Life Cycle and
Prerequisites

Life Cycle Steps

Major Information System

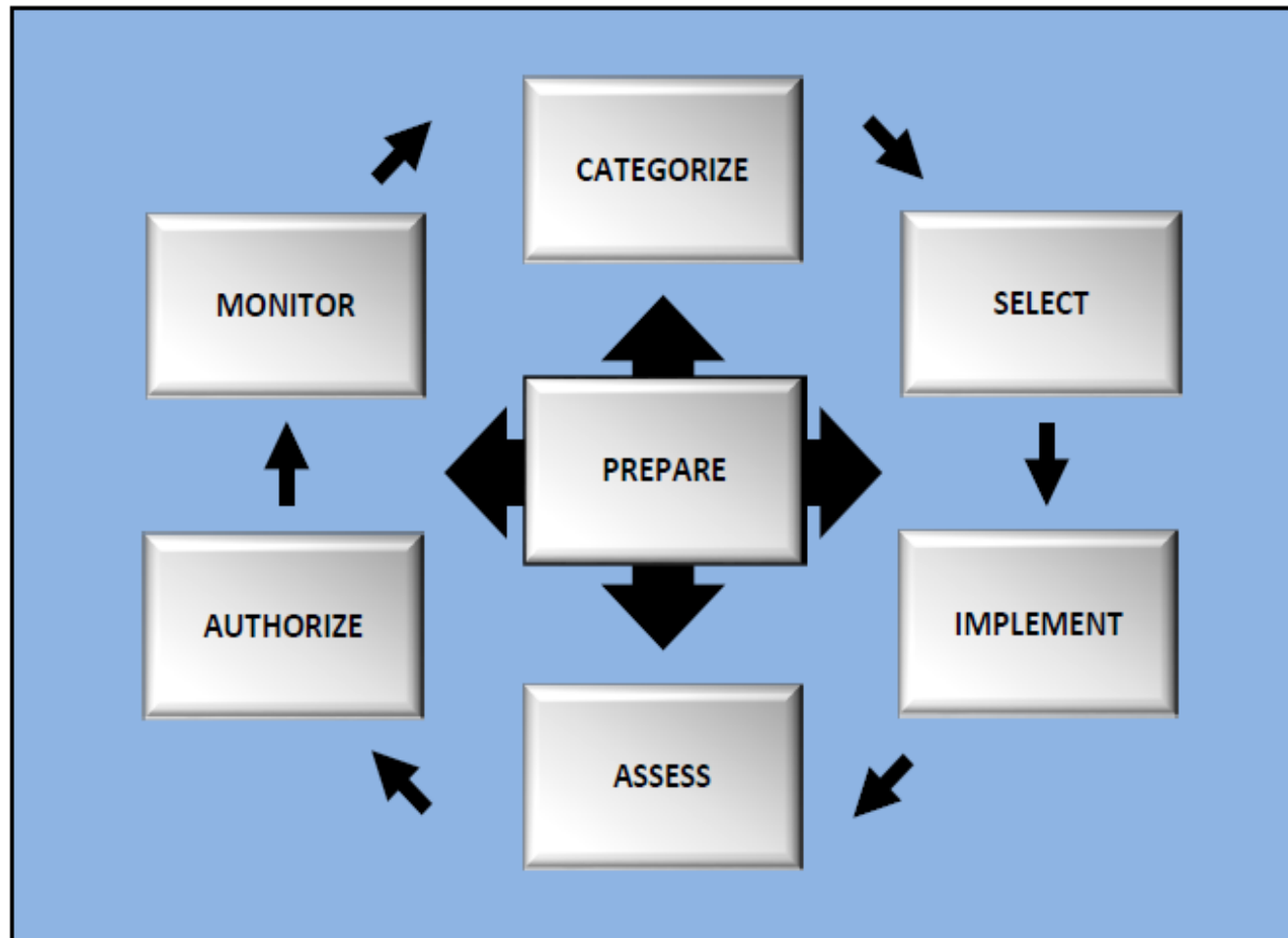
- a system that is part of an investment that requires special management attention as defined in OMB guidance § 2445, or a system that is part of a major acquisition as defined in the OMB Circular A-11, *Capital Programming Guide*, consisting of information resources.⁷² and agency policies, a “major automated information system” as defined in 10 U.S.C. 73

Critical Infrastructure

- systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health safety, or any combination of those matters (42 U.S.C. § 5195c(e))

BAI NIST RMF LIFE CYCLE

- Addition of Preparation Step (NIST SP 800-37 R2):



BAI RMF Prerequisites

- Know the system and environment (information gathering)
 - System name
 - System mission and principal functions
 - Type of information processed and its sensitivity
 - User community
 - System location
 - System components and connectivity
 - System boundary
 - Current authorization status
- Know the players
 - AO (or AO Designated Representative)
 - ISSO
 - Information Owner(s)
 - Other key resources
- Know the requirements
 - “Unique” security requirements
 - Formal or informal risk assessment

BAI NIST SP 800-37 R2 (RMF 2.0)

■ Preparation – Organization requirements

| Tasks | Outcomes |
|---|---|
| TASK P-1 RISK MANAGEMENT ROLES | <ul style="list-style-type: none">Individuals are identified and assigned key roles for executing the Risk Management Framework. [Cybersecurity Framework: ID.AM-6; ID.GV-2] |
| TASK P-2 RISK MANAGEMENT STRATEGY | <ul style="list-style-type: none">A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [Cybersecurity Framework: ID.RM; ID.SC] |
| TASK P-3 RISK ASSESSMENT—ORGANIZATION | <ul style="list-style-type: none">An organization-wide risk assessment is completed or an existing risk assessment is updated. [Cybersecurity Framework: ID.RA; ID.SC-2] |
| TASK P-4 ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL) | <ul style="list-style-type: none">Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [Cybersecurity Framework: Profile] |
| TASK P-5 COMMON CONTROL IDENTIFICATION | <ul style="list-style-type: none">Common controls that are available for inheritance by organizational systems are identified, documented, and published. |
| TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL) | <ul style="list-style-type: none">A prioritization of organizational systems with the same impact level is conducted. [Cybersecurity Framework: ID.AM-5] |
| TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION | <ul style="list-style-type: none">An organization-wide strategy for monitoring control effectiveness is developed and implemented. [Cybersecurity Framework: DE.CM; ID.SC-4] |

NIST SP 800-37 R2 (RMF 2.0)

■ Preparation – System requirements

| Tasks | Outcomes |
|---|---|
| TASK P-8 MISSION OR BUSINESS FOCUS | <ul style="list-style-type: none"> Missions, business functions, and mission/business processes that the system is intended to support are identified. [Cybersecurity Framework: Profile; Implementation Tiers; ID.BE] |
| TASK P-9 SYSTEM STAKEHOLDERS | <ul style="list-style-type: none"> The stakeholders having an interest in the system are identified. [Cybersecurity Framework: ID.AM; ID.BE] |
| TASK P-10 ASSET IDENTIFICATION | <ul style="list-style-type: none"> Stakeholder assets are identified and prioritized. [Cybersecurity Framework: ID.AM] |
| TASK P-11 AUTHORIZATION BOUNDARY | <ul style="list-style-type: none"> The authorization boundary (i.e., system) is determined. |
| TASK P-12 INFORMATION TYPES | <ul style="list-style-type: none"> The types of information processed, stored, and transmitted by the system are identified. [Cybersecurity Framework: ID.AM-5] |
| TASK P-13 INFORMATION LIFE CYCLE | <ul style="list-style-type: none"> All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system. [Cybersecurity Framework: ID.AM-3; ID.AM-4] |
| TASK P-14 RISK ASSESSMENT—SYSTEM | <ul style="list-style-type: none"> A system-level risk assessment is completed or an existing risk assessment is updated. [Cybersecurity Framework: ID.RA; ID.SC-2] |
| TASK P-15 REQUIREMENTS DEFINITION | <ul style="list-style-type: none"> Security and privacy requirements are defined and prioritized. [Cybersecurity Framework: ID.GV; PR.IP] |
| TASK P-16 ENTERPRISE ARCHITECTURE | <ul style="list-style-type: none"> The placement of the system within the enterprise architecture is determined. |
| TASK P-17 REQUIREMENTS ALLOCATION | <ul style="list-style-type: none"> Security and privacy requirements are allocated to the system and to the environment in which the system operates. [Cybersecurity Framework: ID.GV] |
| TASK P-18 SYSTEM REGISTRATION | <ul style="list-style-type: none"> The system is registered for purposes of management, accountability, coordination, and oversight. [Cybersecurity Framework: ID.GV] |

Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework – CSF 2.0)

Table 4. CSF 2.0 Core Function and Category Names and Identifiers


| Function | Category | Category Identifier |
|----------------------|---|---------------------|
| Govern (GV) | Organizational Context | GV.OC |
| | Risk Management Strategy | GV.RM |
| | Cybersecurity Supply Chain Risk Management | GV.SC |
| | Roles, Responsibilities, and Authorities | GV.RR |
| | Policies, Processes, and Procedures | GV.PO |
| | Oversight | GV.OV |
| Identify (ID) | Asset Management | ID.AM |
| | Risk Assessment | ID.RA |
| | Improvement | ID.IM |
| Protect (PR) | Identity Management, Authentication, and Access Control | PR.AA |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Platform Security | PR.PS |
| | Technology Infrastructure Resilience | PR.IR |
| Detect (DE) | Continuous Monitoring | DE.CM |
| | Adverse Event Analysis | DE.AE |
| Respond (RS) | Incident Management | RS.MA |
| | Incident Analysis | RS.AN |
| | Incident Response Reporting and Communication | RS.CO |
| | Incident Mitigation | RS.MI |
| Recover (RC) | Incident Recovery Plan Execution | RC.RP |
| | Incident Recovery Communication | RC.CO |







Fig. 2. Framework Functions

BAI Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework – CSF)

- Emphasis on CSF in the Federal Agency Sector. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) promotes the adoption of CSF.
- Sectors that are participating include Chemical; Defense Industrial Base; Healthcare; Transportation; Water & Wastewater systems; etc.

 An official website of the United States government [Here's how you know](#) ▼





[Services](#)[Report](#)

[Alerts and Tips](#)[Resources](#)[Industrial Control Systems](#)

[Resources](#) > [Cybersecurity Framework](#)

Cybersecurity Framework

[Academia](#)

[Business](#)

[Related Resources](#)

Cybersecurity Framework

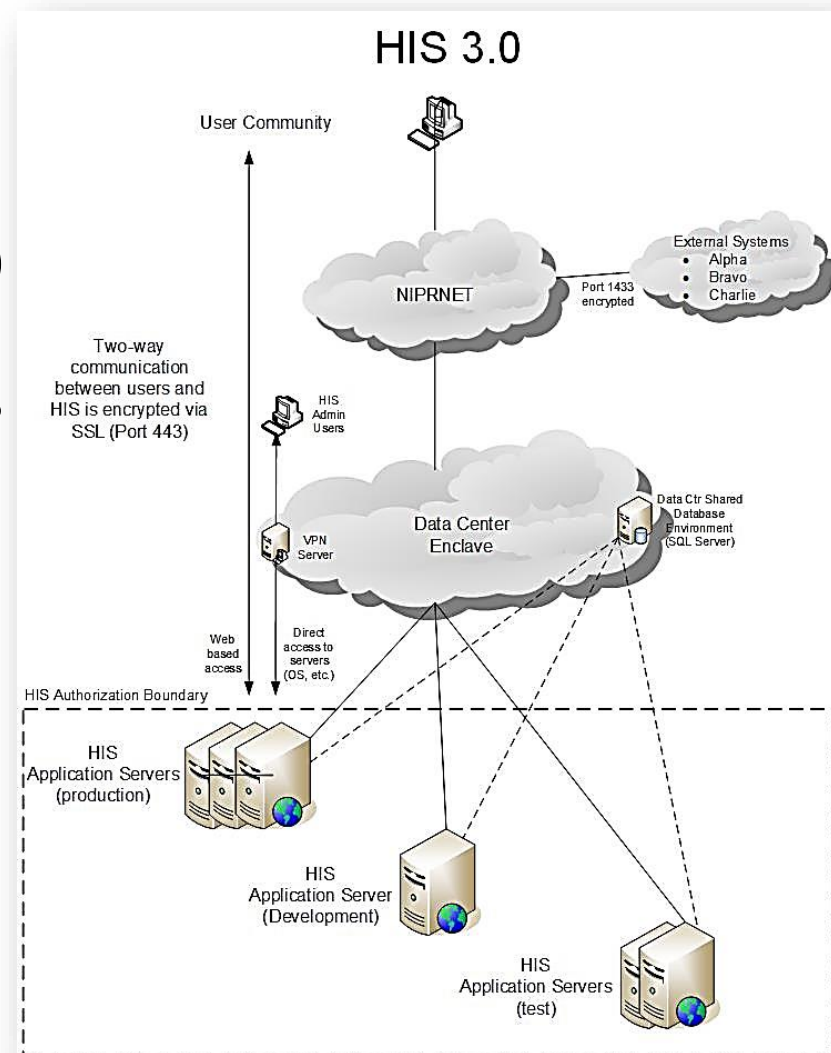
CISA helps organizations use the Cybersecurity Framework to improve cyber resilience. To learn more about the Framework or to download a copy, visit <http://www.nist.gov/cyberframework>. Additionally, visit the links to below for the Microlearn series

CISA connects organizations with public and private sector resources that align to the Framework's five Function Areas: Identify, Protect, Detect, Respond, and Recover. This page explains the Framework Function Areas and provides links to Cybersecurity Framework sector-specific guidance.

<https://us-cert.cisa.gov/resources/cybersecurity-framework>

BAI Prerequisite – System Boundary

- The set of information resources (hardware, software, information, people, etc.) allocated to an IS defines its system (or authorization) boundary
- A well-defined boundary establishes the scope of protection for an IS
- Boundary definition is critical
 - Too expansive → unwieldy risk management process
 - Too restrictive → excessive risk management cost
- Guidelines
 - Direct management control
 - Mission/business objective
 - Operating environment



BAI Step 1 – Categorize Activities



Categorize the System



Information System
Description and Security Plan



Information System
Registration

BAI Security Categorization for non-NSS

- Categorization of Systems is done in accordance with FIPS 199 (Note: Use CNSSI 1253 for NSS)

- Process:

- Analyze the system and determine each of the “information types” processed or stored

- For each information type:

- Use NIST SP 800-60 to obtain an initial categorization
 - Adjust the categorization to account for “special factors”

- For each security objective:

- Select the highest categorization level among all the information types

Information Owner's input is critical

| Info Type | C | I | A |
|---------------------|---|---|---|
| Disaster Prediction | L | H | H |
| Disaster Planning | L | L | L |
| Emergency Response | L | H | H |



System Categorization is:
HIGH

BAI Categorize the System in Accordance with CNSSI 1253 for NSS

- Systems are categorized as High, Moderate or Low for each of the three security objectives (C-I-A)
 - The categorization process is the same as for Non-National Security Systems **EXCEPT** NSS requires impact levels for each security objective

| Info Type | C | I | A |
|---------------------|---|---|---|
| Disaster Prediction | L | H | H |
| Disaster Planning | L | L | L |
| Emergency Response | L | H | H |

System Categorization is:
Confidentiality: LOW
Integrity: HIGH
Availability: HIGH

D.2.1 Border and Transportation Security Information Type

Border and Transportation Security includes facilitating or deterring entry and exit of people, goods, and conveyances at and between U.S. ports of entry, as well as ensuring the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States. Border control involves enforcing the laws regulating the admission of foreign-born persons (i.e., aliens) to the United States. This includes patrolling and monitoring borders and deportation of illegal aliens. Some border control information is also associated with other mission information types (e.g., criminal apprehension, and criminal investigation and surveillance information). In such cases, the impact levels of the associated mission information may determine impact levels associated with border control information. Some aspects of ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States are also covered under the information types associated with the transportation mission. In some cases the border control information may be classified. Any classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified border and transportation security information follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Special Factors Affecting Confidentiality Impact Determination: Where border control information is also associated with other mission information types (e.g., criminal apprehension, and criminal investigation and surveillance information), the confidentiality impact level associated with the information may be **high**. Where unauthorized disclosure of border control information may put the physical safety of personnel into serious jeopardy, the confidentiality impact level associated with the information may be **high**. Unauthorized disclosure of confidentiality of information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States can result in facilitation of terrorist activities that endanger human life. In some cases, the consequent threat to critical infrastructures, key national assets, and human life can be catastrophic. Consequently, the confidentiality impact level associated with information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is normally **high**.

BAI Initiate the Security Plan

NIST SP 800-18

- The Security Plan (SP) is one of three key documents in the Security Authorization Package
- SP is a “living document” revised throughout the RMF life cycle
- SP contains
 - System description (including boundary)
 - List of RMF team members
 - System categorization
 - Security controls
- SP can be maintained “manually” (as a document or spreadsheet) or with an automated tool (i.e., Xacta, eMASS, CSAM, etc.)

BAI Register the System

- Begins by including the system in the Agency IS inventory
- Establishes a relationship between the IS and the parent/governing organization that owns, manages, and/or controls the IS
- Each Agency has its own process for system registration
- Informs the organization of
 - The existence of the IS
 - Key characteristics of the IS
 - Security implications to the organization due to ongoing IS operations
- A system typically receives a registration number that should be recorded in the Security Plan.
- Provides for effective management, accountability, coordination, and oversight of an IS for security status reporting requirements (e.g., laws, policies, etc.)

BAI Step 2 – Select Activities



Common Control Identification



Security Control Selection



Monitoring Strategy



Security Plan Approval

BAI Select Security Controls

- “Catalog” of security controls and control enhancements in NIST SP 800-53 R4

| 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 |

- Three additional Management families in NIST SP 800-53 R5

| | |
|----|---|
| PT | Personally Identifiable Information Processing and Transparency |
| SR | Supply Chain Risk Management |
| PM | Program Management (Driven by Tiers 1 and 2) |

BAI Security Control Example

PE-6 MONITORING PHYSICAL ACCESS

Control:

- a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
- b. Review physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and
- c. Coordinate results of reviews and investigations with the organizational incident response capability.

Note the use of organization-defined values

Discussion: Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as [AU-2](#), if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Related Controls: [AU-2](#), [AU-6](#), [AU-9](#), [AU-12](#), [CA-7](#), [CP-10](#), [IR-4](#), [IR-8](#).

Security Control Example (cont.)

Control Enhancements:

(1) MONITORING PHYSICAL ACCESS | [INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT](#)

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

(2) MONITORING PHYSICAL ACCESS | [AUTOMATED INTRUSION RECOGNITION AND RESPONSES](#)

Recognize [*Assignment: organization-defined classes or types of intrusions*] and initiate [*Assignment: organization-defined response actions*] using [*Assignment: organization-defined automated mechanisms*].

(3) MONITORING PHYSICAL ACCESS | [VIDEO SURVEILLANCE](#)

(a) Employ video surveillance of [*Assignment: organization-defined operational areas*];

(b) Review video recordings [*Assignment: organization-defined frequency*]; and

(c) Retain video recordings for [*Assignment: organization-defined time-period*].

(4) MONITORING PHYSICAL ACCESS | [MONITORING PHYSICAL ACCESS TO SYSTEMS](#)

Monitor physical access to the system in addition to the physical access monitoring of the facility at [*Assignment: organization-defined physical spaces containing one or more components of the system*].

References: None.

Control enhancements are best thought of as simply additional controls.

BAI Select the Control Baseline - NIST vs. CNSS

- Catalog of security controls and control enhancements is in NIST SP 800-53 R4 – Updated to R5 in September 2020
- Non-NSS use SP 800-53B (Control Baselines for Information Systems and Organizations, October 2020) for initial security control baseline

If a Moderate system, select controls in the Moderate column.



| CONTROL NUMBER | CONTROL NAME CONTROL ENHANCEMENT NAME | PRIVACY CONTROL BASELINE | SECURITY CONTROL BASELINES | | |
|----------------|---|--------------------------|----------------------------|-----|------|
| | | | LOW | MOD | HIGH |
| PE-6 | Monitoring Physical Access | | X | X | X |
| PE-6(1) | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT | | | X | X |
| PE-6(2) | AUTOMATED INTRUSION RECOGNITION AND RESPONSES | | | | |
| PE-6(3) | VIDEO SURVEILLANCE | | | | |
| PE-6(4) | MONITORING PHYSICAL ACCESS TO SYSTEMS | | | | X |

BAI Security Control Selection for NSS

Control selection based on system categorization (CNSSI 1253, 29 July 2022)

| ID | Title | Privacy Control Baseline | Privacy Implementation Considerations | Security Control Baselines | | | | | | | | | Justification for NSS | Parameter Value | Tailoring Considerations | | |
|---------|---|--------------------------|---------------------------------------|----------------------------|---|---|---|---|---|---|---|---|-----------------------------------|-----------------|--------------------------|------------|--------|
| | | | | C | | | I | | | A | | | | | Assurance | Resiliency | ATT&CK |
| | | | | L | M | H | L | M | H | L | M | H | | | | | |
| PE-6 | Monitoring Physical Access | | √ _{2,3} | X | X | X | X | X | X | X | X | | b. 1st PV: at least every 90 days | √ | √ | | |
| PE-6(1) | Intrusion Alarms and Surveillance Equipment | | √ _{2,3} | | X | X | | X | X | | X | X | | | √ | | |
| PE-6(2) | Automated Intrusion Recognition and Responses | | | | | | | | | | | | | | √ | √ | |
| PE-6(3) | Video Surveillance | | √ _{2,3} | | | | | | | | | | | | √ | | |
| PE-6(4) | Monitoring Physical Access to Systems | | √ _{2,3} | | | X | | | X | | | X | | | √ | √ | |

- Assurance is a measure of confidence in the security or privacy capability provided by the control.
- Resiliency is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption.
- MITR ATT&CK – Website knowledge base of adversary tactics and techniques; control has ability to respond to adversary tactics and techniques.

BAI Common Control Identification

- System Owner is responsible for identifying each baseline security control as one of:
 - System specific control – Implemented by the system owner within the system boundary
 - Common control – Implemented outside the system boundary by another organization (“Common Control Provider”) and is “inherited”
 - Hybrid control – Partially inherited, partially implemented by the system owner
- Common Controls can be leveraged (inherited) by multiple IS
- Examples: A data center’s physical, environmental and network controls; Organizational policies and procedures maintained by an agency or component
- Common Control Providers must be assessed to verify that common controls are in place and operating correctly
- System Owner is responsible for ensuring agreements (e.g., MOA) between Common Control Provider and inheriting IS

BAI Apply Tailoring Process

- The initial security control baseline can be “tailored” in numerous ways
 - Inserting organization-defined values into the controls where required
 - Specifying compensating controls when implementation of the control “as written” would be impractical or prohibitively expensive
 - Applying scoping guidance to declare certain controls as “Not Applicable” or include unique organizational requirements
 - Supplementing the baseline with controls to address “unique” security requirements
 - The Security Plan should be revised to reflect the tailored baseline (including appropriate justification)

BAI Security Control Overlays

- The purpose of Security Control Overlay is to tailor the baseline “in one fell swoop” rather than one control at a time
- Specific “communities of interest” are developing overlays to address their specific needs
- CNSS reviews overlays and post on their website www.cnss.gov
- Currently available CNSS overlays include:
 - Classified systems
 - Privacy (PII, PHI)
 - Space Platform
 - Intelligence
 - Cross-domain solutions
- Additional Overlays available:
 - Operational Technology (Industrial control) systems (NIST SP 800-82 R3)
 - Finance
 - Insider Threat (National Geospatial-Intelligence Agency)

NOTE : CNSSI 1253 Appendix F1 contains a template for overlay development

“Unclassified//For Official Use Only”
(UNCLASSIFIED//FOUO) are available on the restricted CNSS website.

Develop System-level Continuous Monitoring Strategy

- Continuous monitoring strategy should include:
 - Monitoring effectiveness of security controls (including inherited controls)
 - Monitoring of actual and proposed changes to the IS
 - Annual review of controls (and independence of assessor)
 - Periodic reporting of security status to AO
- Continuous monitoring strategy should be included in the SP (explicitly or by reference)
- NIST SP 800-137 is currently the best available reference on this subject
- Additional policies and guidance on Continuous Monitoring are anticipated

Review and Approve Security Plan and Continuous Monitoring Strategy

- AO (or designated rep) reviews and approves the SP
- Approval signals AO's concurrence with
 - System boundary
 - System categorization
 - Security control baseline, tailoring and overlays
 - Monitoring strategy
- AO approval should be documented in the SP

Each Agency may have its own process for submitting the SP for AO approval

BAI Step 3 – Implement Activities



Implement control solutions consistent with enterprise and information security architectures



Document security control implementation in the security plan

BAI Implement Controls

- Security controls are implemented as part of system buildout
- Information Security Architect and Engineer are key players
- Common controls leveraged to the greatest extent possible
- Implementation must include configuring of products in accordance with approved applicable standardized configuration guidance (e.g., National Checklist Repository in the NIST national vulnerability data base; DISA Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) Benchmarks, etc.)

Self-Assessment – Verification of Control Implementation

- CISA provides tools for Federal Agency self-assessment:
 - Cybersecurity Evaluation Tool (CSET)
 - Self-use tool that includes security assessments & network verification/scanning tools
 - Cyber Resilience Review (CRR)
 - Recommended for critical infrastructures used with Cybersecurity Framework
 - <https://www.cisa.gov/resources/federal>

BAI Document Security Control Implementation in the SP

- Update SP as controls are implemented
- For common controls, system owner should verify that Common Control Provider is compliant

SECURITY PLAN

- Implementation statements
- Reference documentation artifacts that support control implementation

BAI Step 4 – Assess Activities



Develop, Review and Approve Security Assessment Plan



Assess Security Controls



SCA Prepares Security Assessment Report (SAR)



Conduct Initial Remediation Actions

BAI Develop and Approve Security Assessment Plan

- RMF requires “independent assessment” to verify implementation of security controls
- Contents: means by which each control in the baseline will be assessed:
 - Examine
 - Interview
 - Test
- Sources: NIST SP 800-53A Rev4 – R5 now published
- Prepared by the Security Control Assessor (SCA)*
- Reviewed/approved by AO

* Each Agency is responsible for developing its own “independent assessment” process

Assessment Procedure Example

| PE-06 | MONITORING PHYSICAL ACCESS | |
|-------|--|---|
| | ASSESSMENT OBJECTIVE: <i>Determine if:</i> | |
| | PE-06_ODP[01] | <i>the frequency at which to review physical access logs is defined;</i> |
| | PE-06_ODP[02] | <i>events or potential indication of events requiring physical access logs to be reviewed are defined;</i> |
| | PE-06a. | physical access to the facility where the system resides is monitored to detect and respond to physical security incidents; |
| | PE-06b.[01] | physical access logs are reviewed <PE-06_ODP[01] frequency>; |
| | PE-06b.[02] | physical access logs are reviewed upon occurrence of <PE-06_ODP[02] events>; |
| | PE-06c.[01] | results of reviews are coordinated with organizational incident response capabilities; |
| | PE-06c.[02] | results of investigations are coordinated with organizational incident response capabilities. |
| | POTENTIAL ASSESSMENT METHODS AND OBJECTS: | |
| | PE-06-Examine | [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; physical access monitoring records; physical access log reviews; system security plan; other relevant documents or records]. |
| | PE-06-Interview | [SELECT FROM: Organizational personnel with physical access monitoring responsibilities; organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities]. |
| | PE-06-Test | [SELECT FROM: Organizational processes for monitoring physical access; mechanisms supporting and/or implementing physical access monitoring; mechanisms supporting and/or implementing the review of physical access logs]. |

BAI Assess Security Controls

- Assessment activities are conducted in accordance with the Security Assessment Plan, which entails:
 - Executing assessment procedures as documented in NIST SP 800-53A
 - Assessing IT products for compliance with standardized configurations; as required
 - Verifying inherited controls with Common Control Providers
- Each control in the approved baseline is assessed as Satisfied (S), Other than Satisfied (O), or Not Applicable (NA)
- Assessment activities may be conducted on-site, remotely, or a combination of both

BAI SCA Prepares Security Assessment Report (SAR)

- SAR content for each control
 - Description of assessment procedure and result
 - Satisfied/Other than Satisfied/Not Applicable
- SAR content for each “O” control
 - Supporting data showing which portion(s) of the control were not compliant and why
 - Potential for compromise of security objectives
 - Recommended mitigation
- Assessment of overall (aggregate) system risk
- Additional information/recommendations

BAI Conduct Initial Remediation Actions

- Having received the SAR, the System Owner may choose to address some or all the Other than Satisfied (O) controls “immediately” and request reassessment
- Reassessed controls should be so noted in the SAR

BAI Step 5 – Authorize Activities



Prepare the POA&M



Submit Security Authorization Package (security plan, SAR and POA&M) to AO



AO conducts final risk determination



AO makes risk acceptance (authorization) decision

BAI Prepare the POA&M

- System Owner prepares a Plan of Action and Milestones (POA&M) in response to the findings in the SAR
- For each finding, the POA&M details
 - Planned remediation steps
 - Resources required
 - Milestones and scheduled completion dates
- POA&M is maintained throughout the system life cycle
 - Items are updated to show correction or mitigation, but not removed
- Vulnerabilities in inherited (common) controls must be tracked on the POA&M
- POA&Ms are monitored and tracked by:
 - AO
 - SISO

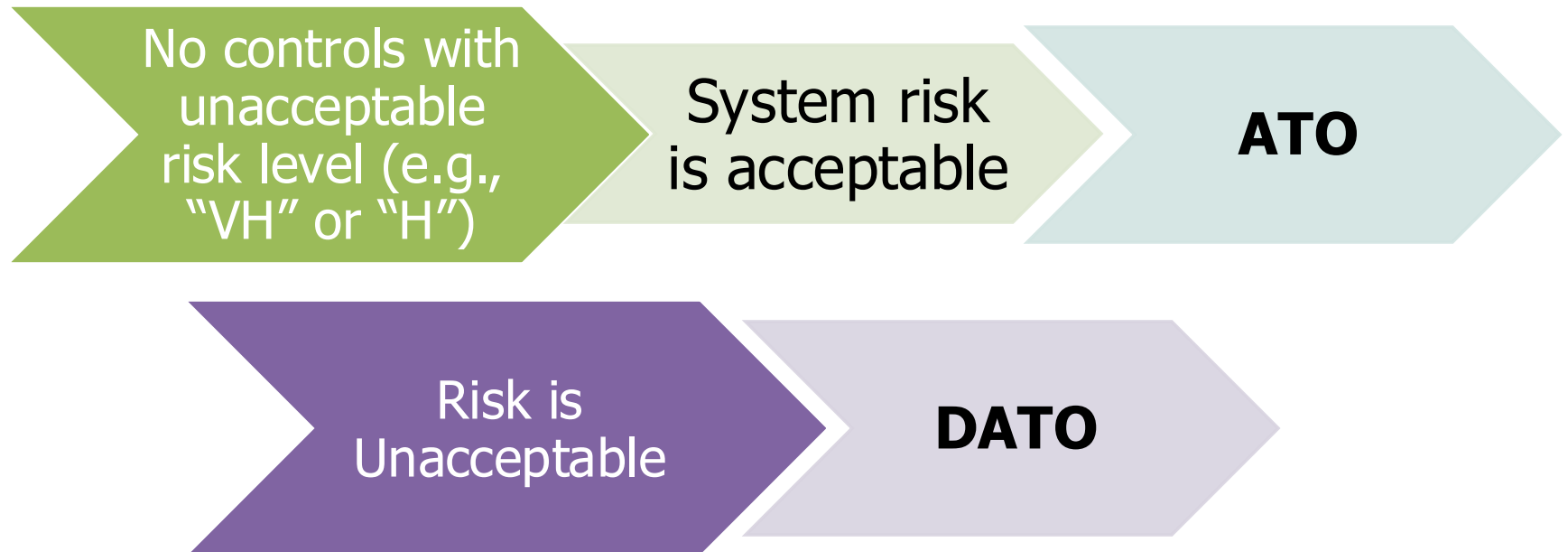
BAI Submit Security Authorization Package to AO

- Security Authorization Package consists of the SP, SAR and POA&M
- Package is assembled by System Owner or ISSO and sent to the AO (or via the AODR) for review and approval

BAI AO Makes Authorization Decision

- Basis of authorization decision
 - Are there any Other than Satisfied (O) controls with an unacceptable risk level (e.g., Very High (VH) or High (H))?
 - Is the overall system risk acceptable?
- Potential authorization decisions
 - Authorization to Operate (ATO)
 - Denial of Authorization to Operate (DATO)
 - Some organizations may have authorization decisions that are used internally:
 - Interim Authorization to Test (IATT)
 - ATO with conditions

BAI Authorization Decision Process



BAI Authorization Decisions

■ ATO

- AO must specify an Authorization Terminate Date (ATD) of 3 years or less
- Continuous monitoring → “Ongoing authorization”?
 - Robust continuous monitoring program in place
 - Supporting reporting requirements

■ DATO

- If system is currently operational, it must be disconnected

AO electronically communicates signed authorization decision to System Owner (e.g., via Xacta, eMASS, etc.)

BAI Type Authorization

- Used to deploy identical copies of an IS in specified environments
- A single Security Authorization Package is developed and approved for “archetype” version of the system
- System is deployed along with installation, security control and configuration requirements, and operational security needs to be provided by the hosting enclave
- AOs of hosting enclaves must approve installation of the system into their boundary

- Used to streamline acceptance of “deploying systems” with valid authorization into “receiving organizations”
- Receiving organization
 - Reviews the security authorization package
 - Determines security impact of connecting the deploying system within the receiving enclave
 - Determines risk of hosting the deploying system
 - Documents acceptance by the receiving AO
 - Updates its authorization to show inclusion of the deployed system

BAI Step 6 – Monitor Activities



Determine impact of changes to the system and environment



Assess selected controls annually
Conduct needed remediation
Update security plan, SAR and POA&M



Report security status to AO
AO reviews reported status



Implement system decommissioning strategy

BAI Maintaining Security Posture Over Time

- Effective change management is essential
- Show current changes:
 - Performance monitoring
 - Periodic independent evaluations
- Proposed changes
 - Change, Configuration and Patch Management processes

BAI Assess Selected Controls Annually

- Assess a subset of controls in accordance with the approved Continuous Monitoring Strategy
- Assess remainder of controls annually per FISMA
- Determine risk responses
- Update RAR and POA&M
- Assessor reports to AO
- AO reviews
- AO can determine “ongoing authorization” based on maturity of continuous monitoring strategy

AO may downgrade or revoke authorization decision if risk conditions so warrant

BAI Remediate, Document, Report, Review

- Remediate: Remediation activities continue throughout the life cycle in response to:
 - POA&M items
 - Ongoing monitoring activities
 - Periodic assessments of risk
- Document: System owner and ISSO ensure Authorization Package (SP, SAR, POA&M) is kept up-to-date
- Report: Security status reported to AO in accordance with approved continuous monitoring strategy
- Review: AO reviews status reports to determine if risk remains acceptable

DHS CISA Continuous Monitoring in Federal Agencies

- Continuous Diagnostics and Mitigation (CDM)
 - Provides federal agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize and mitigate most significant problems first
 - <https://www.cisa.gov/securing-federal-networks>
- EINSTEIN
 - Used by agencies across the Federal Civilian Executive Branch (FCEB). EINSTEIN detects and block cyberattacks from compromised federal agencies.
 - <https://www.cisa.gov/einstein>
- Quality Services Management Office Marketplace (QSMO)
 - Provides cyber services for purchase by agencies to help manage risks
 - <https://www.cisa.gov/cyber-qsmo-marketplace>

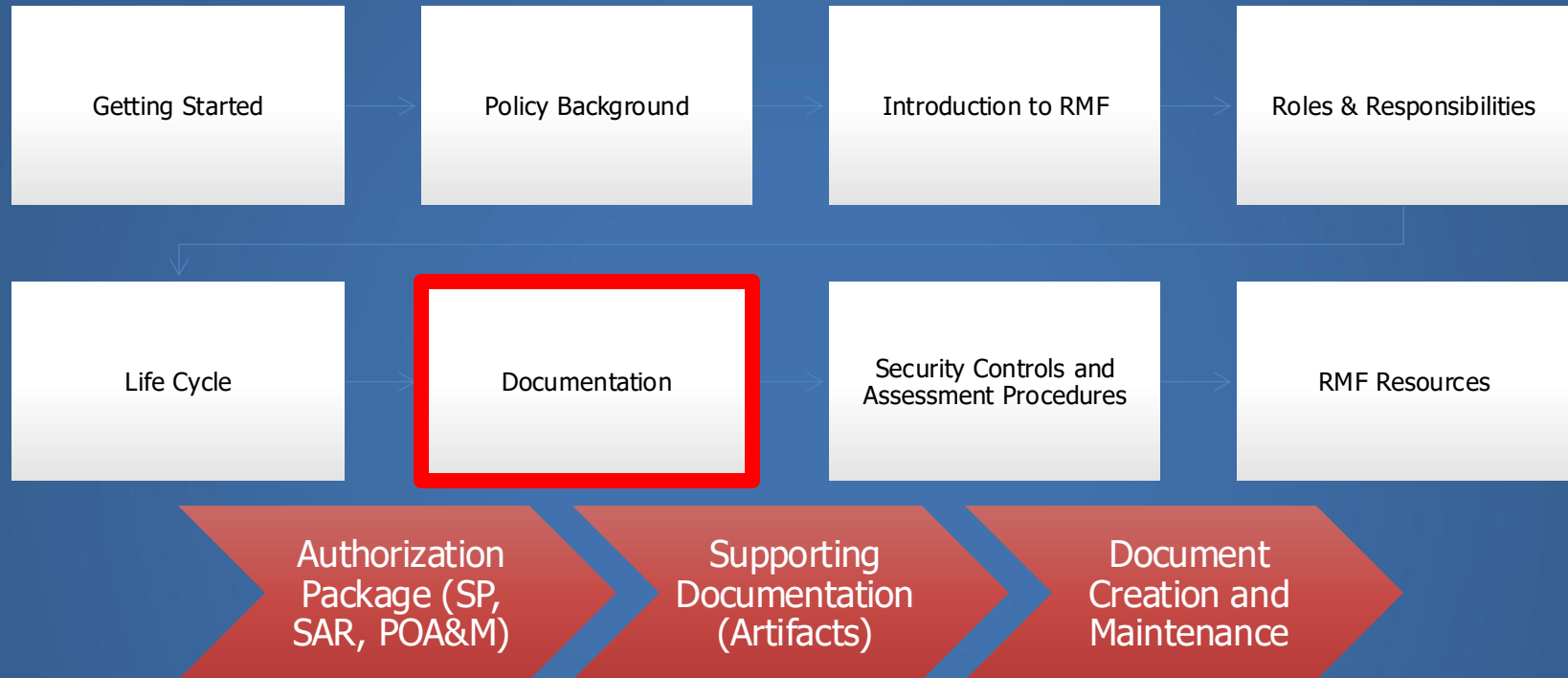
BAI Continuous Monitoring and Reassessment

- Previously, systems were required to be reassessed and reauthorized at least once every 3 years
- Focus of OMB Circular A-130 (2016) is Ongoing Authorization
 - Complete an initial authorization (utilizing NIST RMF)
 - Transition to an ongoing authorization process utilizing Information System Continuous Monitoring (ISCM) strategy
 - Reauthorize based on time or event basis in accordance with agency risk tolerance
- Replaces previous 3-yr authorization
 - AO receives necessary & sufficient information regarding security & privacy state of system to determine risk acceptability

BAI Implement System Decommissioning Strategy

- Decommissioning strategy should include
 - Dealing with inheritance relationships
 - Final SP update
 - Removal of system from tracking databases
 - Secure disposal of documentation artifacts

- All IT Systems require authorization
- Prerequisites to RMF include understanding the system (especially the system boundary) and key players
- RMF life cycle consists of these major steps:
 - Prepare
 - Categorize
 - Select
 - Implement
 - Assess
 - Authorize
 - Monitor



BAI Authorization Package

- RMF Authorization Package consists of
 - Security Plan (SP)
 - Security Assessment Report (SAR)
 - Plan of Action and Milestones (POA&M)
 - Other required documentation

SP Content

- System information
- RMF team members
- Categorization
- Security control baseline (including overlays and tailoring)
- Implementation and status of each control

SAR Content

- Assessment results for each control (S, O, NA)
- For O controls:
 - Risk level
 - Recommended mitigation
- Overall system risk level

POA&M Content

- For each "weakness"
 - Description
 - Risk level
 - Associated controls
 - Planned remediation
 - Resources
 - Milestones
 - Estimated completion
 - Status

Supporting Artifacts Are Not a Required Part of Authorization Package

- Assessor MAY Review to Verify Control Implementation...
- Artifacts provide evidence that security controls and control enhancements have been implemented as required

Policies

"This is what we do."

Procedures
(SOPs)

"This is how we do it."

Assurance
Docs

"See? We're actually doing it!"

- Implementation descriptions in SP should refer to appropriate supporting artifact(s)
- Tools (e.g., Xacta, CSAM, eMASS) provide
 - Repository for artifacts
 - Ability to enter artifact references into control implementation descriptions in SP

Artifacts are not part of the Authorization Package *per se*, but they are reviewed by the assessor to verify control implementation

BAI Document Creation and Maintenance

- Word documents / Excel spreadsheets
 - Prevalent method in many federal civil agencies
 - Documents can be very lengthy
 - Some templates are available (e.g., Security Plan template in NIST SP 800-18)
- Automated tools (e.g., Xacta, eMASS, CSAM, CSET, etc.)

Other Options for Federal Agencies Security Plan

- Build SP utilizing template provided in the NIST SP 800-18.
- Build SP utilizing the Department of Justice Cyber Security Asset Management (CSAM) tool, a web-based network capability to assess, document, manage and report on the status of IT security controls.

<https://www.justice.gov/jmd/cybersecurity-services>

NIST Special Publication 800-18
Revision 1

NIST

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

Guide for Developing Security Plans for Federal Information Systems

Marianne Swanson
Joan Hash
Pauline Bowen

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006



System Security Plan - Example

| | | | | |
|---|-------|------------|-------------------|--------------|
| System Security Plan Federal Organization | | | | |
| 1. Information System Name/Title | | | | |
| This document presents the System Security Plan (SSP) for the FedOrg Enterprise System (FES). | | | | |
| 2. Information System Categorization | | | | |
| | Low | X | Moderate | High |
| Table 1 Categorizaation | | | | |
| 3. Information System Owner | | | | |
| Name | Title | Agency | Email | Phone |
| John Cromwell | CIO | Fed Agency | jcromwell@fed.gov | 222-211-1200 |
| Table 2 System Owner | | | | |
| 4. Authorizing Official | | | | |
| Name | Title | Agency | Email | Phone |
| Tiffany Wright | DAA | Fed Agency | twright@fed.gov | 222-211-1211 |
| Table 3 Authorizing Official | | | | |
| 5. Other Designated Contacts | | | | |
| Name | Title | Agency | Email | Phone |
| Michelle Ace | CA | Fed Agency | mace@fed.gov | 222-211-1203 |
| Table 4 Desiganted Contacts | | | | |

BAI System Security Plan - Example

6. Assignment of Security Responsibility:

- Name, title, address, email address, and phone number of person who is responsible for the security of the system.

7. Information System Operational Status:

- Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

| | | | | | |
|--------------------------|-------------|--------------------------|-------------------|--------------------------|--------------------|
| <input type="checkbox"/> | Operational | <input type="checkbox"/> | Under Development | <input type="checkbox"/> | Major Modification |
|--------------------------|-------------|--------------------------|-------------------|--------------------------|--------------------|

8. Information System Type:

- Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 9. General System Description/Purpose.

| | | | |
|--------------------------|-------------------|--------------------------|------------------------|
| <input type="checkbox"/> | Major Application | <input type="checkbox"/> | General Support System |
|--------------------------|-------------------|--------------------------|------------------------|

9. General System Description/Purpose

- Describe the function or purpose of the system and the information processes.

| |
|--|
| |
|--|

BAI System Security Plan - Example

10. System Environment

- Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.



11. System Interconnections/Information Sharing

- List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

| System Name | Organization | Type | Agreement (ISA/MOU/MOA) | Date | FIPS 199 Category | C&A Status | Auth. Official |
|-------------|--------------|------|-------------------------|------|-------------------|------------|----------------|
| | | | | | | | |

12. Related Laws/Regulations/Policies

- List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

BAI System Security Plan - Example

13. Minimum Security Controls

The following section provides a thorough description of how the minimum security controls in the applicable baseline are being implemented (in-place) or planned to be implemented. The controls are described by control family and will indicate whether it is a system control, hybrid control, common control, scoping guidance is applied, or a compensating control is being used as applicable.

13.1 Access Control (AC)

13.2 (AC-1) Access control Policy and Procedures

a. Security Control

The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

b. Status – Planned

Formal access controls procedures have not been developed. The Owner is ultimately responsible for ensuring FES access control policies and procedures are in place. The Owner has delegated the responsibility for developing the policies and procedures to the CIO.

c. Planned Activities

BAI Security Assessment Report (SAR)

- One of three key documents in the security authorization package
- Provides the results of the Security Control Assessment (SCA) with recommendations for corrective actions for weaknesses or deficiencies
 - Sometimes known as Security Test and Evaluation (ST&E)
- Information is provided on the effectiveness of controls within or inherited by the IS
 - Validates the status (i.e., Planned, In Place, Not Applicable) for each control or enhancement
 - Assists the AO in risk determination and acceptance decisions
- NIST SP 800-53A provides guidance for assessing each of the security controls in SP 800-53

BAI Security Assessment Report – NIST SP 800-53A

| CP-3 CONTINGENCY TRAINING | | |
|---|---|---|
| ASSESSMENT OBJECTIVE: <i>Determine if the organization provides contingency training to information system users consistent with assigned roles and responsibilities:</i> | | |
| CP-3(a) | CP-3(a)[1] | <i>within the organization-defined time period of assuming a contingency role or responsibility; (S)</i> |
| | CP-3(a)[2] | <i>defines a time period within which contingency training is to be provided to information system users assuming a contingency role or responsibility; (S)</i> |
| CP-3(b) | <i>when required by information system changes; (O)</i> | |
| CP-3(c) | CP-3(c)[1] | <i>thereafter, in accordance with the organization-defined frequency; (S)</i> |
| | CP-3(c)[2] | <i>defines the frequency for contingency training. (S)</i> |
| Comments and Recommendations: CP-3(b) is marked as <i>other than satisfied</i> because assessors could not find evidence that the organization provided contingency training to information system users consistent with their assigned roles and responsibilities when there were significant changes to the system. | | |



Plan of Action and Milestone (POA&M)

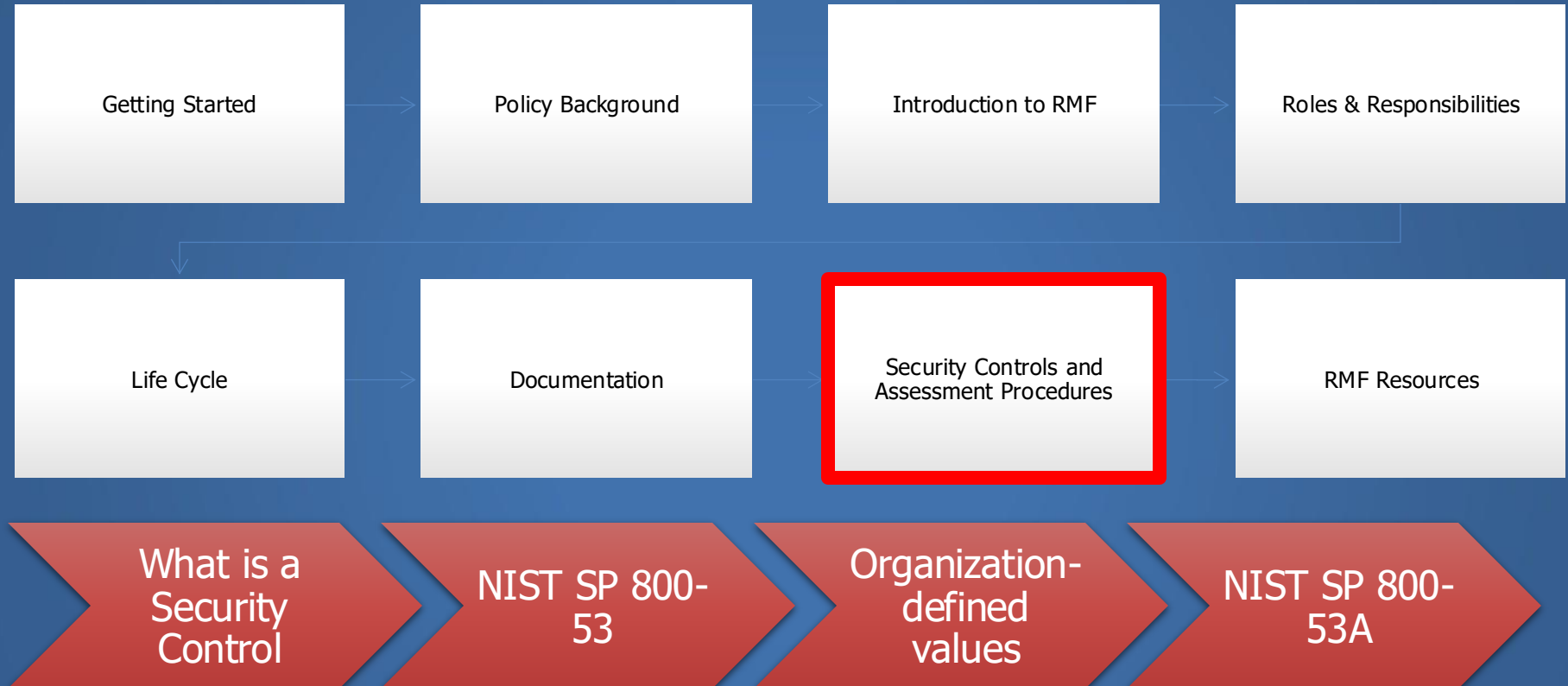
Sample System-level Security Plan of Action and Milestones

| Weaknesses | POC | Security Control | Scheduled Completion Date | Milestones with Completion Dates | Milestone Changes | Identified in CFO Audit or other review? | Status |
|---|-------------------------------|------------------|---------------------------|---|-------------------|--|-----------|
| 1 -- Password controls improperly configured and not tested | Program office | IA-5(1) | 10/1/01 | Reconfigure and test password controls -- 10/1/01 | | Yes | Completed |
| 2 -- Security plan is out of date, more than one year since last update despite new interconnections | Program office | PL-2 | 11/30/01 | Update plan and obtain independent review -- 11/30/01 | | No | Ongoing |
| 3 -- System vulnerabilities have not been periodically tested as specified in OMB policy and Security Act | Program office and agency CIO | RA-5 | 1/15/02 | Arrange for system vulnerability testing -- 10/15/01 | | Yes | Ongoing |

BAI Other Documentation Considerations

- Accessibility
- Version control, check-in/check-out, etc.
- Information sensitivity
- Document marking

- RMF Authorization Package consists of: Security Plan, Security Assessment Report, POA&M
- Additional supporting documentation (artifacts) required as evidence of control implementation (compliance)
- SP, SAR and POA&M can be developed and maintained in several ways
 - Word documents (not recommended)
 - Automated tool such as CSAM, eMASS, Xacta
- Accessibility, version control, information sensitivity and document marking need to be considered



BAI What is a Security Control?

- Concise statement of a specific security capability (i.e., safeguard/countermeasure) needed to protect a particular aspect of an IS
- Security control characteristics
 - Objective condition should be testable
 - Compliance should be measurable
 - Activities required to achieve the Control should be assignable, and therefore accountable

“Security Control” ↔ “Security Requirement”

Catalog of Controls – NIST SP 800-53 R4 moving to R5 in the future

BAI

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

April 2013

INCLUDES UPDATES AS OF 01-22-2015

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

September 2020

INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

JOINT TASK FORCE

Family Changes:

- 20 total families
 - Integrates Privacy within other families - only one Privacy-pure family
 - Personally Identifiable Information Processing and Transparency (PT)
 - Program Management family
 - Adds several new Program Management (PM) controls to address Privacy
 - New Supply Chain Risk Management family (SR)

NIST SP 800-53 R5 – Personally Identifiable Information Processing and Transparency (PT)

| CONTROL NUMBER | CONTROL NAME CONTROL ENHANCEMENT NAME |
|-------------------------|---|
| PT-1 | Policy and Procedures |
| PT-2 | Authority to Process Personally Identifiable Information |
| PT-2(1) | DATA TAGGING |
| PT-2(2) | AUTOMATION |
| PT-3 | Personally Identifiable Information Processing Purposes |
| PT-3(1) | DATA TAGGING |
| PT-3(2) | AUTOMATION |
| PT-4 | Consent |
| PT-4(1) | TAILORED CONSENT |
| PT-4(2) | JUST-IN-TIME CONSENT |
| PT-4(3) | REVOCAION |
| PT-5 | Privacy Notice |
| PT-5(1) | JUST-IN-TIME NOTICE |
| PT-5(2) | PRIVACY ACT STATEMENTS |
| PT-6 | System of Records Notice |
| PT-6(1) | ROUTINE USES |
| PT-6(2) | EXEMPTION RULES |
| PT-7 | Specific Categories of Personally Identifiable Information |
| PT-7(1) | SOCIAL SECURITY NUMBERS |
| PT-7(2) | FIRST AMENDMENT INFORMATION |
| PT-8 | Computer Matching Requirements |

BAI NIST SP 800-53 R5 – Program Management (PM)

| CONTROL NUMBER | CONTROL NAME CONTROL ENHANCEMENT NAME |
|--------------------------|--|
| PM-1 | Information Security Program Plan |
| PM-2 | Information Security Program Leadership Role |
| PM-3 | Information Security and Privacy Resources |
| PM-4 | Plan of Action and Milestones Process |
| PM-5 | System Inventory |
| PM-5(1) | INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION |
| PM-6 | Measures of Performance |
| PM-7 | Enterprise Architecture |
| PM-7(1) | OFFLOADING |
| PM-8 | Critical Infrastructure Plan |
| PM-9 | Risk Management Strategy |
| PM-10 | Authorization Process |
| PM-11 | Mission and Business Process Definition |
| PM-12 | Insider Threat Program |
| PM-13 | Security and Privacy Workforce |
| PM-14 | Testing, Training, and Monitoring |
| PM-15 | Security and Privacy Groups and Associations |
| PM-16 | Threat Awareness Program |
| PM-16(1) | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE |
| PM-17 | Protecting Controlled Unclassified Information on External Systems |
| PM-18 | Privacy Program Plan |
| PM-19 | Privacy Program Leadership Role |

Expanded to include several privacy controls.

| | |
|--------------------------|---|
| PM-20 | Dissemination of Privacy Program Information |
| PM-20(1) | PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES |
| PM-21 | Accounting of Disclosures |
| PM-22 | Personally Identifiable Information Quality Management |
| PM-23 | Data Governance Body |
| PM-24 | Data Integrity Board |
| PM-25 | Minimization of Personally Identifiable Information Used in Testing, Training, and Research |
| PM-26 | Complaint Management |
| PM-27 | Privacy Reporting |
| PM-28 | Risk Framing |
| PM-29 | Risk Management Program Leadership Roles |
| PM-30 | Supply Chain Risk Management Strategy |
| PM-30(1) | SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS |
| PM-31 | Continuous Monitoring Strategy |
| PM-32 | Purposing |

NIST SP 800-53 R5 – Supply Chain Risk Management (SR)

| CONTROL NUMBER | CONTROL NAME CONTROL ENHANCEMENT NAME | |
|--------------------------|---|--|
| SR-1 | Policy and Procedures | |
| SR-2 | Supply Chain Risk Management Plan | |
| SR-2(1) | ESTABLISH SCRM TEAM | |
| SR-3 | Supply Chain Controls and Processes | |
| SR-3(1) | DIVERSE SUPPLY BASE | |
| SR-3(2) | LIMITATION OF HARM | |
| SR-3(3) | SUB-TIER FLOW DOWN | |
| SR-4 | Provenance | |
| SR-4(1) | IDENTITY | |
| SR-4(2) | TRACK AND TRACE | |
| SR-4(3) | VALIDATE AS GENUINE AND NOT ALTERED | |
| SR-4(4) | SUPPLY CHAIN INTEGRITY — PEDIGREE | |
| SR-5 | Acquisition Strategies, Tools, and Methods | |
| SR-5(1) | ADEQUATE SUPPLY | |
| SR-5(2) | ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE | |
| SR-6 | Supplier Assessments and Reviews | |
| SR-6(1) | TESTING AND ANALYSIS | |
| SR-7 | Supply Chain Operations Security | |
| SR-8 | Notification Agreements | |
| SR-9 | Tamper Resistance and Detection | |
| SR-9(1) | MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE | |
| SR-10 | Inspection of Systems or Components | |
| SR-11 | Component Authenticity | |
| SR-11(1) | ANTI-COUNTERFEIT TRAINING | |
| SR-11(2) | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR | |
| SR-11(3) | ANTI-COUNTERFEIT SCANNING | |
| SR-12 | Component Disposal | |

- Content Changes
 - Contains information on controls for all federal agencies and supporting contractors
 - Baseline control selection process depends on the organization and will be addressed in other publications
 - Controls written more proactively (outcome-based) and include all types of platforms such as general purpose, closed, mobile, industrial control and Internet of Things (IoT)* devices
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations – published October 2020 – addresses Federal agency baselines (Note: NSS will continue to use CNSSI 1253.)



Example Control from Rev 5

Control ID
and Title

Control
Text

Discussion

Control
Enhancements

- Number
- Title
- Text
- Supplemental
- Guidance

References

No Baseline

Moved to SP 800-53B

IR-3 INCIDENT RESPONSE TESTING

Control: Test the effectiveness of the incident response capability for the system [*Assignment: organization-defined frequency*] using the following tests: [*Assignment: organization-defined tests*].

Discussion: Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Related Controls: [CP-3](#), [CP-4](#), [IR-2](#), [IR-4](#), [IR-8](#), [PM-14](#).

Control Enhancements:

(1) INCIDENT RESPONSE TESTING | [AUTOMATED TESTING](#)

Test the incident response capability using [*Assignment: organization-defined automated mechanisms*].

Discussion: Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities. This can be accomplished by providing more complete coverage of incident response issues, selecting realistic test scenarios and environments, and stressing the response capability.

Related Controls: None.

(2) INCIDENT RESPONSE TESTING | [COORDINATION WITH RELATED PLANS](#)

Coordinate incident response testing with organizational elements responsible for related plans.

Discussion: Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

Related Controls: None.

(3) INCIDENT RESPONSE TESTING | [CONTINUOUS IMPROVEMENT](#)

Use qualitative and quantitative data from testing to:

- (a) Determine the effectiveness of incident response processes;
- (b) Continuously improve incident response processes; and
- (c) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

Discussion: To help incident response activities function as intended, organizations may use metrics and evaluation criteria to assess incident response programs as part of an effort to continually improve response performance. These efforts facilitate improvement in incident response efficacy and lessen the impact of incidents.

Related Controls: None.

References: [\[OMB A-130\]](#), [\[SP 800-84\]](#), [\[SP 800-115\]](#).

NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53Ar5>

| | | |
|-------|---|--|
| IR-03 | INCIDENT RESPONSE TESTING | |
| | ASSESSMENT OBJECTIVE: <i>Determine if:</i> | |
| | IR-03_ODP[01] | <i>frequency at which to test the effectiveness of the incident response capability for the system is defined;</i> |
| | IR-03_ODP[02] | <i>tests used to test the effectiveness of the incident response capability for the system are defined;</i> |
| | IR-03 | the effectiveness of the incident response capability for the system is tested <IR-03_ODP[01] frequency> using <IR-03_ODP[02] tests>. |
| | POTENTIAL ASSESSMENT METHODS AND OBJECTS: | |
| | IR-03-Examine | [SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; privacy plan; other relevant documents or records]. |
| | IR-03-Interview | [SELECT FROM: Organizational personnel with incident response testing responsibilities; organizational personnel with information security and privacy responsibilities]. |

BAI Organization-defined Values

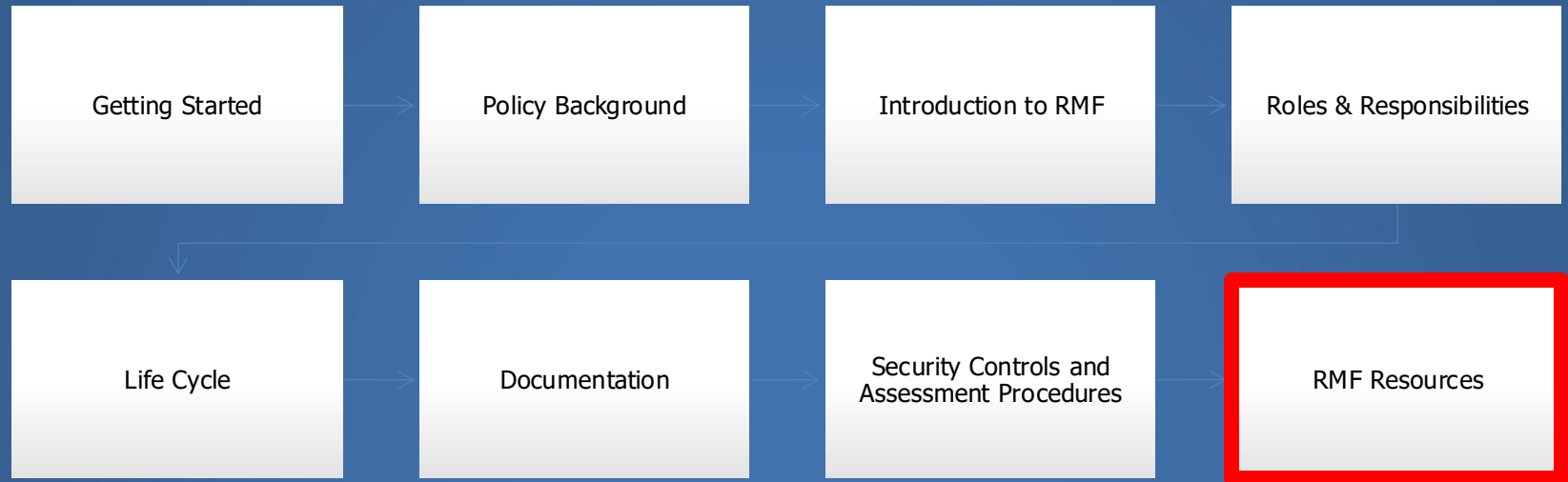
MP-7 MEDIA USE

Control:

- a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and
- b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

- Types of organization-defined values
 - Assignment: "fill in the blank"
 - Selection: "multiple choice"
- How to determine
 - Agency Policy & Guidance
 - System Owner's Discretion
 - Best Practices
- Sources
 - Agency Standards & Procedures
 - CNSSI 1253

- Security control is a concise statement of a specific safeguard or countermeasure
- FIPS 200 provides information on security control families
- For NSS, security control baseline is selected in accordance with CNSSI 1253
- NIST SP 800-53 R4/5 contains the “catalog” of security controls used in the RMF process
- NIST security controls make liberal use of organization-defined values
- NIST SP 800-53A R4/5 contains the assessment objectives and methods for each of the controls and control enhancements



Projects

Publications

Topics

News & Updates

Events

Glossary

About CSRC

+

+



NIST REVISES MEASUREMENT GUIDE FOR
INFORMATION SECURITY



CPRT: CYBERSECURITY AND PRIVACY
REFERENCE TOOL



REVIEW AND COMMENT ON OUR DRAFT
PUBLICATIONS

+

The **Computer Security Resource Center (CSRC)** has information on many of NIST's cybersecurity- and information security-related projects, publications, news and events. CSRC supports people and organizations in government, industry, and academia—both in the U.S. and internationally.

- Learn more about [current projects](#) and [upcoming events](#)
- Search and browse our [publications library](#) of current and historical standards, guidelines, and other reports
- Explore content by [topic](#)
- Search our [glossary](#) of terms defined in our publications
- Subscribe to [CSRC email updates](#)

FEATURED LINKS

Crypto Module Validation Program
& Validated Modules Search

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

Projects

Publications

Drafts for Public Comment

NIST Special Publications (SPs)

FIPS

NIST Internal/Interagency Reports (NISTIRs)

ITL Bulletins

Topics

Publications

NIST develops and maintains an extensive collection of standards, guidelines, recommendations, and research on the security and privacy of information and information systems. This includes various NIST technical publication series:

FIPS

Federal Information Processing Standards: Security standards.

SP

NIST Special Publications

Guidelines, technical specifications, recommendations and reference materials, comprising multiple sub-series:

SP 800

Computer security

SP 1800

Cybersecurity practice guides

SP 500

Information technology (relevant documents)

NISTIR

NIST Internal or Interagency Reports

Reports of research findings, including background information

NIST CSRC – Subscribe for Updates



HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

[Contact Us](#) | [Our Other Offices](#)



Want updates about CSRC and our publications? [Subscribe](#)

Send inquiries to csrc-inquiry@nist.gov

[Site Privacy](#) | [Accessibility](#) | [Privacy Program](#) | [Copyrights](#) | [Vulnerability Disclosure](#) | [No Fear Act Policy](#) | [FOIA](#) | [Environmental Policy](#) | [Scientific Integrity](#) |

[Information Quality Standards](#) | [Commerce.gov](#) | [Science.gov](#) | [USA.gov](#) | [Vote.gov](#)

The screenshot shows the NIST CSRC 'Email Updates' form. At the top is the NIST logo. The form title is 'Email Updates'. Below it is a sub-header: 'To sign up for updates or to access your subscriber preferences, please enter your contact information below.' The form contains two main fields: 'Subscription Type' with a dropdown menu currently set to 'Email', and 'Email Address' with a text input field. Below these fields are 'SUBMIT' and 'CANCEL' buttons. A small line of text below the buttons reads: 'Your contact information is used to deliver requested updates or to access your subscriber preferences.' At the bottom of the form are links for 'Privacy Policy' and 'Help'.

Recommended!

BAI Subscription Topics

Subscription Topics

☐ Information Technology Laboratory (ITL)

☐ ITL Bulletin

☐ ITL Newsletter

☐ Health IT

☐ Cybersecurity Programs

☐ Computer Security Resource Center (CSRC) Website

☒ Draft Publications (includes FIPS, SPs, NISTIRs) [i](#)

☒ Federal Information Processing Standards (FIPS) [i](#)

☒ Special Publications (SPs) [i](#)

☒ NIST Interagency Reports (NISTIRs) [i](#)

☒ ITL Security Bulletins [i](#)

☒ Announcements [i](#)

☒ NIST Cybersecurity Events [i](#)

☐ Federal Information Security Management Act (FISMA) Project

☐ Trusted Identities Group (TIG)

☐ National Initiative for Cybersecurity Education (NICE)

☒ NICE [i](#)

☒ NICE eNewsletter [i](#)

☒ NICE Webinars [i](#)

☒ Cybersecurity Framework

☒ Cybersecurity Framework Updates

☐ National Cybersecurity Center of Excellence (NCCoE)

☐ Usable Cybersecurity

Submit

Cancel

☐ Federal Information Security Management Act (FISMA) Project

☐ Trusted Identities Group (TIG)



The screenshot shows the CNSS website interface. At the top is a dark navigation bar with the CNSS logo on the left and links for ABOUT, LIBRARY, HELP, LOGIN YOUR ACCOUNT, and SEARCH. Below the navigation bar is a large banner image. On the left of the banner is a woman in a military uniform holding a folder. The background of the banner is an aerial view of a large, modern building complex with a digital overlay of numbers. The text "Committee on National Security Systems" is centered over the banner in large white font. Below the banner is a solid blue bar with the text "Meeting Current and Future Threats" in white. A small CNSS logo is visible in the bottom right corner of the banner image.

Committee on National Security Systems

Meeting Current and Future Threats

<https://www.cnss.gov>

BAI CNSSI 1253 and Overlays

[CNSSI 1253E Attachment 1](#)

Security Overlays Template

Release Date: 12/12/2022, File Size: 283020

Updated to reflect NIST SP 800-53 Rev. 5 and the corresponding update to CNSSI 1253.

[CNSSI 1253E Attachment 3](#)

Cross Domain Solution Overlay

Release Date: 02/08/2023, File Size: 1284227

Updated to reflect NIST SP 800-53 Rev. 5 and the corresponding update to CNSSI 1253.

This document is designated FOUO. To access protected FOUO content in the CNSS Library, you must login with a Federal/DoD Public Key Infrastructure (PKI), Personal Identity Verification (PIV) or Common Access Card (CAC) client certificate correctly installed in your browser and click on the "CAC/PKI/PIV Login" button above.

[CNSSI 1253E, Attachment 5](#)

Classified System Overlay

Release Date: 09/30/2022, File Size: 553253

This overlay identifies security control specifications needed to safeguard classified information stored, processed, or transmitted by national security systems (NSS). Updated to reflect NIST SP 800-53 Rev. 5 and the corresponding update to CNSSI 1253.

[CNSSI 1253F - Attachment 2](#)

Space Platform Overlay

Release Date: 02/23/2018, File Size: 541790

Administrative changes from Rev 3 to Rev 4.

[CNSSI 1253F Attachment 4](#)

Intelligence Overlay

Release Date: 04/19/2016, File Size: 511613

This document is designated FOUO. To access protected FOUO content in the CNSS Library, you must login with a Federal/DoD Public Key Infrastructure (PKI), Personal Identity Verification (PIV) or Common Access Card (CAC) client certificate correctly installed in your browser and click on the "CAC/PKI/PIV Login" button above.


[CNSSI 1253F, Attachment 6](#)

Privacy Overlay

Release Date: 04/23/2015, File Size: 1035048

This document is comprised of four Privacy Overlays that identify security and privacy control specifications required to protect personally identifiable information (PII), including protected health information (PHI), in National Security Systems (NSS) and reduce privacy risks to individuals throughout the information lifecycle.








BAI Department of Homeland Security (DHS)




Homeland Security


Official website of the Department of Homeland Security

Contact Us



Topics | News | In Focus | [How Do I?](#) | Get Involved | About DHS

Enter Search Term | On DHS.gov | 


 > Topics

Topics

- Border Security
- Citizenship and Immigration
- Cybersecurity
- Disasters
- Economic Security
- Election Security
- Homeland Security Enterprise
- Human Trafficking
- Immigration and Customs Enforcement
- Preventing Terrorism
- Resilience
- Science and Technology
- Transportation Security


Topics

Below are a variety of topics handled by the Department of Homeland Security.




Border Security

Protecting our borders from the illegal movement of weapons, drugs, contraband, and people, while promoting lawful trade and travel, is essential to homeland security, economic prosperity, and national sovereignty.




Citizenship and Immigration Services

Managed by U.S. Citizenship and Immigration Services (USCIS), the United States' lawful immigration system is one of the most generous in the world.



Cybersecurity

Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.



Disasters

Whatever the disaster, the Federal Emergency Management Agency, or FEMA, leads the federal government's response as part of a team of responders.

<https://www.dhs.gov/topics>



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**

[COVID Questions](#)[Report Cyber Issue](#)[CYBERSECURITY](#)[INFRASTRUCTURE
SECURITY](#)[EMERGENCY
COMMUNICATIONS](#)[NATIONAL RISK
MANAGEMENT](#)[ABOUT
CISA](#)[MEDIA](#)

CYBERSECURITY

CISA leads the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life.

Quick Links

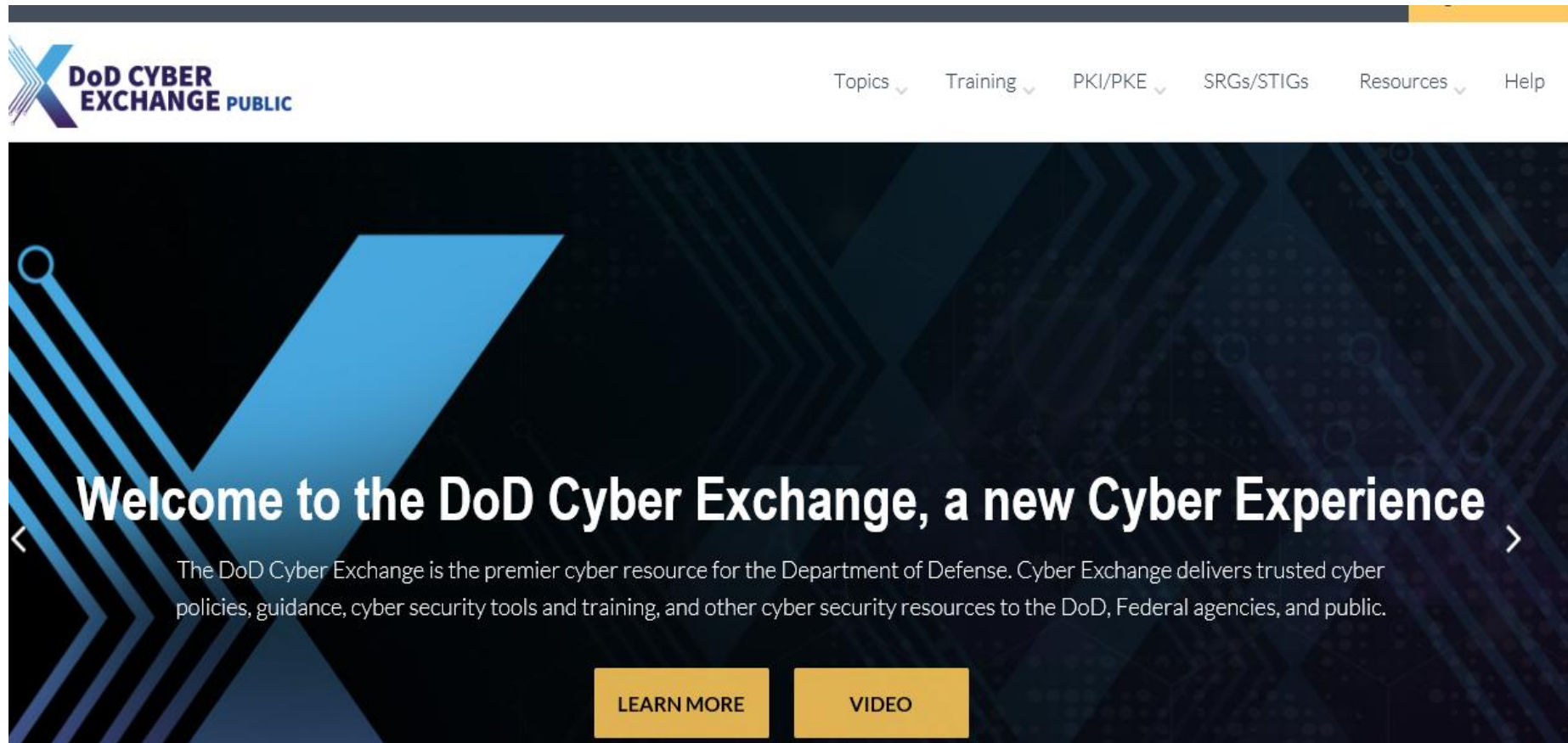
- [CISA Insights](#)
- [Combating Cyber Crime](#)
- [Coordinated Vulnerability Disclosure](#)
- [Cyber Essentials](#)
- [Cyber Incident Response](#)
- [Cyber Safety](#)
- [Cyber Resource Hub](#)

- [Supply Chain Compromise](#)
- [Cybersecurity Governance](#)
- [Cybersecurity Insurance](#)
- [Cybersecurity Training & Exercises](#)
- [Detection and Prevention](#)
- [Education](#)
- [Cyber EO 14028](#)

- [Ransomware Guidance and Resources](#)
- [Cyber Hygiene Services](#)
- [Information Sharing](#)
- [Protecting Critical Infrastructure](#)
- [Securing Federal Networks](#)
- [Shop Safely](#)

<https://www.cisa.gov/cybersecurity>

BAI DoD Cyber Exchange (previously DISA IASE)



DoD Cyber Exchange Public (<https://public.cyber.mil>)
or
DoD Cyber Exchange CAC Holder (<https://cyber.mil>)

BAI DoD Cyber Exchange – STIGs



[Topics](#) [Training](#) [PKI/PKE](#) [SRGs/STIGs](#) [Resources](#) [Help](#)

Security Technical Implementation Guides (STIGs)

[SRG/STIGs Home](#)

[Control Correlation Identifier \(CCI\)](#)

[Document Library](#)

[DoD Annex for NIAP Protection Profiles](#)

[DoD Cloud Computing Security](#)

STIGs

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

[View and Download STIGs](#)

Some Federal Agencies now use the Cyber Exchange Security Implementation Guides (STIGS) to provide configuration requirements for automated systems.

BAI Commercial Automated Applications

Commercial software applications can assist in information gathering, workflow tracking, document preparation, and other aspects of RMF



<https://www.telos.com/>

- NIST Computer Security Resource Center (CSRC) website contains a plethora of RMF information and an extensive document library
- CNSS website is the source of approved security control overlays
- Cyber Exchange website is the source of technical configuration guidance (STIGs)
- DHS assists with implementation of information security policies for federal systems, including providing technical assistance and providing deploying technologies

- This course was designed to help you be able to:
 - Describe the fundamental concepts of information security and risk management
 - Describe relevant information security policies and guidance (e.g., FISMA, FIPS Publications, NIST Special Publications, CNSS Publications)
 - Summarize the key RMF roles and responsibilities
 - Describe the major life cycle steps of the Risk Management Framework
 - Recall the key documents comprising the RMF “authorization package”
 - Generalize the purpose and organization of the NIST Security Controls and Assessment Procedures
 - Identify the primary online resources supporting RMF

BAI Thank you for attending!

You Can Rest Easy



With a Strong Security Program

BAI Information Security
Consulting & Training

RMF Resource Center

1-800-RMF-1903

<https://rmf.org>

E-mail: rmf@rmf.org

Please email us. We'd love to hear from you!