



The slide features a background image of a globe with a checkered floor and a colorful, swirling energy field. A white box in the center contains the title "RISK MANAGEMENT FRAMEWORK (RMF) for DoD IT *Fundamentals* v9.0". The BAI logo is in the bottom left, and the page number "1" is in the bottom right.

**RISK MANAGEMENT FRAMEWORK
(RMF) for DoD IT *Fundamentals* v9.0**

BAI Information Security
Consulting & Training
© 2024

1

1



The slide is titled "Getting Started" in red. It features a grid of eight white boxes with blue borders, arranged in two rows of four. The first box in the top row, "Getting Started", is highlighted with a red border. Below the grid are four red chevron arrows pointing right, each containing text. The BAI logo is in the top left, and the page number "2" is in the bottom right.

BAI Information Security
Consulting & Training

Getting Started

Getting Started	Policy Background	Introduction to RMF	Roles & Responsibilities
Life Cycle	Documentation	Security Controls and NIST SP 800-53 R5 Transition	RMF Resources

Background, Problem, Solution and Target Audience

Class Schedule and Classroom Logistics

Course Scope and Learning Objectives

Information Security Concepts

© 2024

2

2

BAI Background

- 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 “civil” departments/agencies
 - Intelligence community
 - DoD
- DoD began (March 2014) a process of transition from its legacy risk management process (DIACAP) to RMF

© 2024

3

3

BAI Solution

- This class will provide you with high-level knowledge of:
 - The Risk Management Framework (RMF)
 - Implementation of RMF in the DoD environment (“RMF for DoD IT”)
 - RMF Resources – websites, publications, automated tools

© 2024

4

4

BAI Target Audience

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

© 2024

5

5



Meet Your Course Developer...

BAI Information Security Consulting and Training
 "Risk Management Framework Resource Center"

<https://rmf.org>

Follow us on LinkedIn and join our group!

"Risk Management Framework Resource Center"



© 2024

6

6

BAI Information Security
Consulting & Training

Meet Your
Course Leader




© 2024 7

7

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



© 2024 8

8

BAI This Class

- RMF for DoD IT Fundamentals is a one-day standalone course
- Also, first day of a four-day program:
RMF for DoD IT 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
- Additional one-day add-ons; e.g., eMASS Essentials; STIG 101 (online)
- Class format: Lecture and discussion

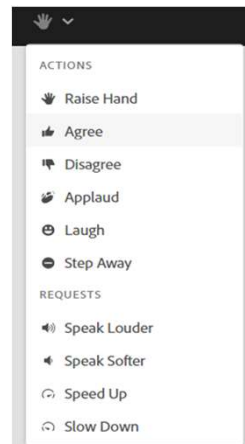
© 2024

9

9

BAI Getting Started

- | | |
|--|---|
| <ul style="list-style-type: none"> ■ Traditional Classroom <ul style="list-style-type: none"> ■ Building security, badges, etc. ■ Restrooms ■ Refreshments ■ Lunch suggestions ■ Internet access ■ Course Materials: <ul style="list-style-type: none"> ■ Onsite students receive a hard-copy version of the slides ■ Online students receive a pdf file of today's class slides:
DA1-RMF for DoD IT Fundamentals | <ul style="list-style-type: none"> ■ Online Classroom <ul style="list-style-type: none"> ■ Audio options ■ Chat box ■ Document box |
|--|---|



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

© 2024

10

10

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

© 2024

11

11

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, DoD Policy Documents)
 - 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 RMF for DoD IT

© 2024

12

12

BAI The Basics: Terminology

Information
Security

Information
Assurance

Cybersecurity

Same or different?

© 2024

13

13

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. Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity.
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

© 2024

14

14

BAI Information Security Concepts

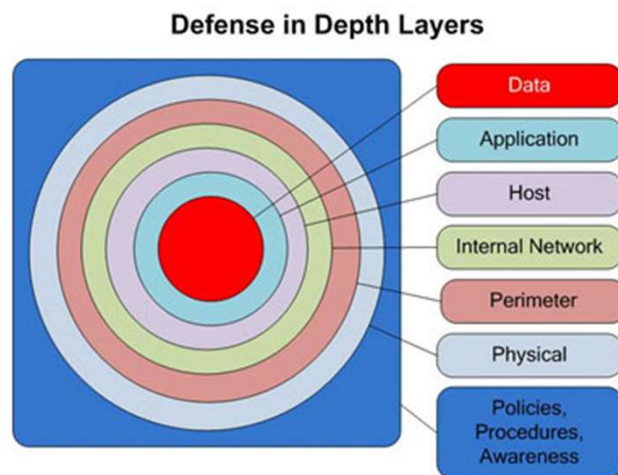
- Effective information security:
 - People
 - Process
 - AND Tools
 - Goes beyond physical equipment and software that is processing the data
- Successfully protecting information means understanding multiple technical and non-technical security disciplines
- “Holistic view” of the information system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

© 2024

15

15

BAI Defense-in-Depth



© 2024

16

16

BAI Holistic View

Source: NIST SP 800-53 R4

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

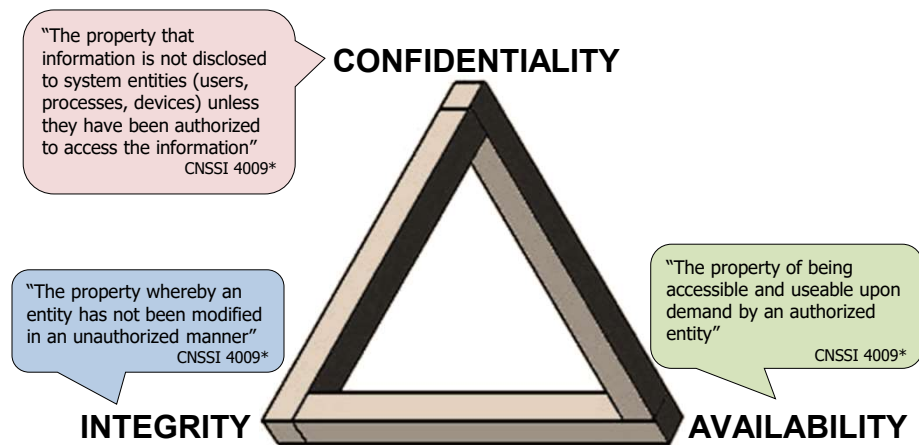
© 2024

17

17

BAI Security Objectives

Fundamental Principles of Information Security



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

© 2024

18

18

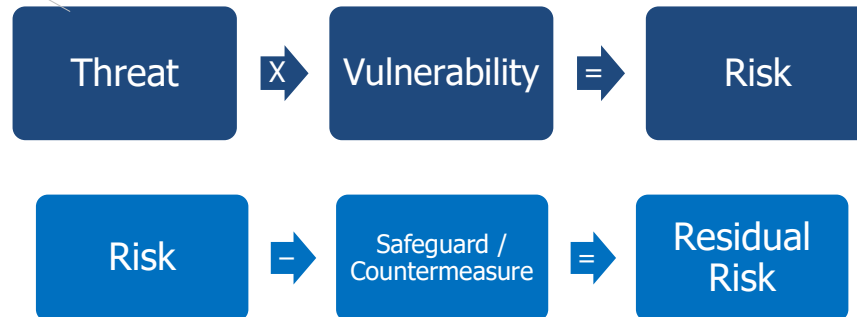
BAI Risk Management Model

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
3. Defect in software code exploited when patching is not current.



© 2024

19

19

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

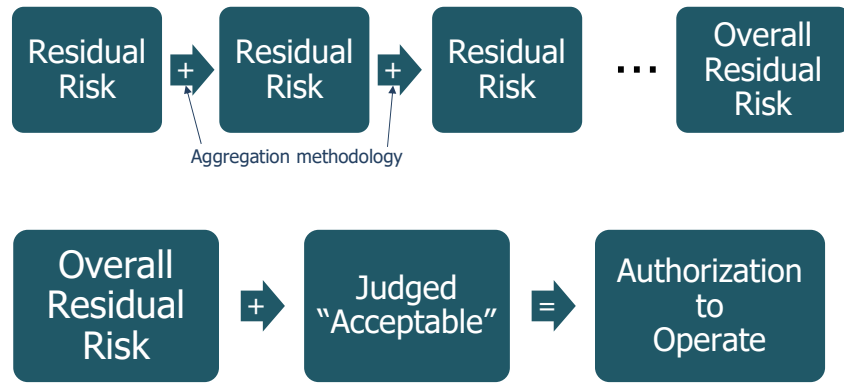
Source: NIST Special Publication 800-30

© 2024

20

20

BAI Acceptance of Risk



© 2024

21

21

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?

© 2024

22

22

BAI Note to Contractors

- Contractors must build and maintain systems in accordance with DoD standards
- However, the government is ultimately responsible for accepting the risk and authorizing the system for operation

© 2024

23

23

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.



© 2024

†

24

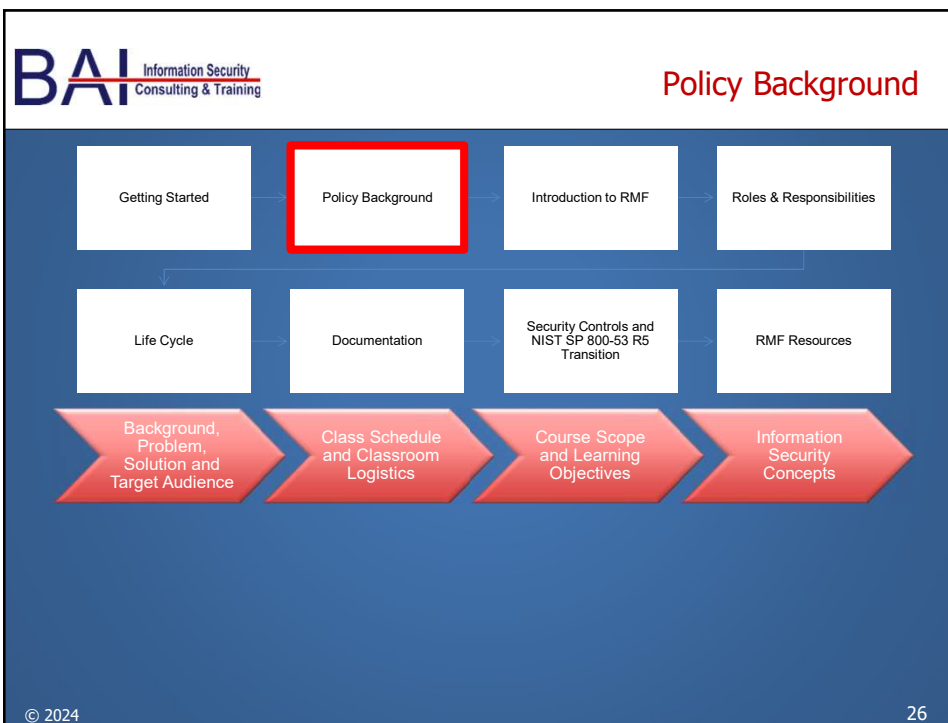
BAI Review

- 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 should embrace the concept of “defense in depth”
- 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

© 2024

25

25



© 2024

26

26

BAI FISMA



- 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 "Civil" 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.*

© 2024

27

27

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

© 2024

28

28

BAI FISMA 2014

- 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.**

© 2024

29

29

BAI 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)

© 2024

30

30

BAI National Institute of Standards and Technology (NIST)

- 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

© 2024 31

31

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

© 2024 32

32

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.

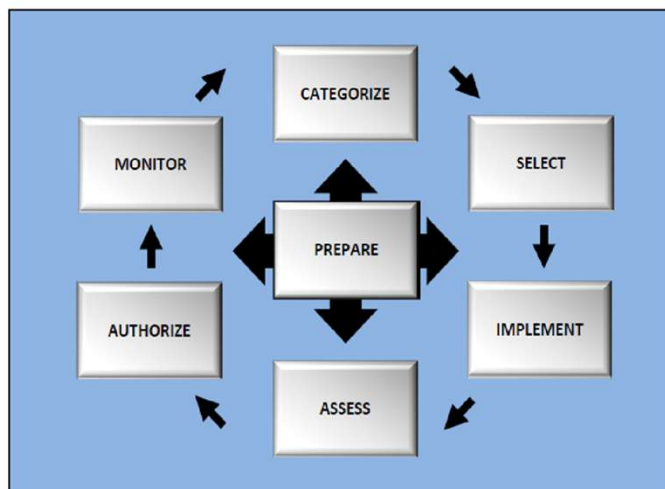
© 2024

33

33

BAI NIST RMF LIFE CYCLE

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



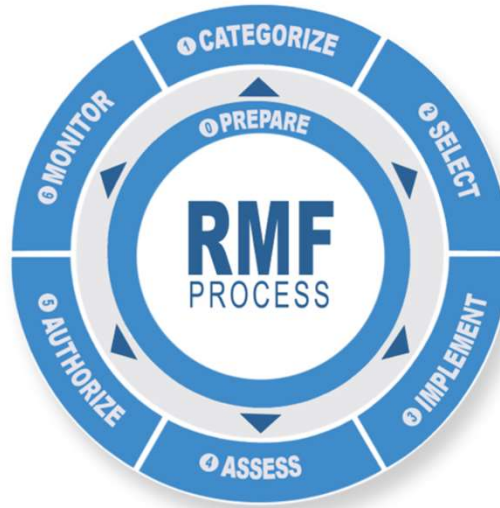
© 2024

34

34

BAI DoD RMF LIFE CYCLE

- Addition of Preparation Step (DoD 8510.01):



© 2024 Source: RMF Knowledge Service

35

35

BAI NIST SP 800-37 R2 (RMF 2.0)


- 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

© 2024

36

36

BAI Committee on National Security Systems (CNSS)
Instructions 1253 & 1254



- 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 (New update July 2022)
 - 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

© 2024 37

37

BAI What is a National Security System?

- National Security Systems (NSS) are information systems operated by USG, 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); or
 - are critical to the direct fulfillment of military or intelligence missions (not including routine administrative and business applications)
- Are all DoD systems considered NSS?
 - NO!
 - HOWEVER,... DoD has made a policy decision to treat all systems as if they were NSS for the purpose of security authorization (i.e., RMF)
- What does this mean?
 - It means CNSSI 1253 is applicable to all DoD systems, regardless of whether they are NSS or not!

Note: Outside of DoD (e.g., in federal civil agencies), CNSSI 1253 applies only to systems designated as NSS

Resource: NIST SP 800-59, Guidelines for Identifying an Information System as a National Security System
© 2024 38

38

BAI DoD Publications – DoDI 8500.01

- Supersedes DoDI 8500.1 – Information Assurance
- Rescinds DoDI 8500.2 – Information Assurance Implementation
- New terminology and new names for key roles
- Some new roles and responsibilities
- Describes the 3-tier approach to risk management
- Describes the various types of DoD IT



Department of Defense
INSTRUCTION

NUMBER 8500.01
March 14, 2014

DoD CIO

SUBJECT: Cybersecurity

© 2024

39

39

BAI DoD Publications – DoDI 8510.01

- DoDI 8510.01 – previously DIACAP, now RMF (New update July 2022)
- Establishes RMF as DoD's "enterprise-wide decision structure for cybersecurity risk management" consistent with NIST SP 800-37
- Guidelines for transitioning from DIACAP to RMF
- Promotes cybersecurity reciprocity and continuous monitoring
- All DoD systems must:
 - Be categorized in accordance with CNSSI 1253
 - Use security controls from NIST SP 800-53
 - Use assessment procedures from NIST SP 800-53A

Certification & Accreditation → Assessment & Authorization



Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014

DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

© 2024

40

40

BAI DoD Policies (DoDI 8510.01)

- "Implement to the greatest extent possible"
 - Reciprocal acceptance of DoD and other federal agency authorizations
 - Continuous monitoring capabilities
- "Resources for implementing RMF must be identified and allocated as part of the budgeting process"

© 2024

41

41


BAI Key RMF Related Pubs

NIST Special Publication 800-37
Revision 2


**Risk Management Framework for
Information Systems and Organizations**

A System Life Cycle Approach for Security and Privacy

CNSSI No. 1253
29 July 2022



**CATEGORIZATION AND CONTROL
SELECTION FOR
NATIONAL SECURITY SYSTEMS**



DoD INSTRUCTION 8510.01

RISK MANAGEMENT FRAMEWORK FOR DoD SYSTEMS

Originating Component: Office of the DoD Chief Information Officer

Effective: July 19, 2022

Releasability: Cleared for public release. Available on the Directives Division Website at <https://www.esd.whs.mil/DD>.

© 2024

42

42

BAI So that's it... Just two DoD pubs?

- Well ... not quite! Other DoD pubs are alive and well!
 - DoDD 8140.01 Cyberspace Workforce Management (replaces 8570)
 - DoDI 8580.1 – Information Assurance (IA) in the Defense Acquisition System
 - DoDI 8551.1 – Ports, Protocols and Services Management
 - DISA Security Technical Implementation Guides (STIGs), Security Requirements Guides (SRGs)
 - ... and many, many, more

Expect these documents to also be revised in the future, at a minimum to embrace new RMF terminology.

© 2024

43

43

BAI Summary

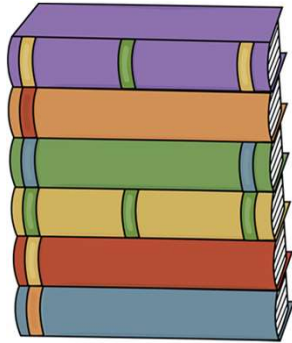
- RMF for DoD IT relies on publications from several government entities
- FISMA is the overarching legislation
- OMB Circular A-130 introduced the concept of system authorization
- NIST publishes a large library of RMF guidance documents (Special Publications) for adoption/adaptation by agencies, as well as a smaller number of FIPS Publications, which are mandatory
- CNSSI 1253 is applicable to all DoD systems (as well as National Security Systems in other agencies)
- The principal RMF-related DoD documents are DoDI 8500.01 (Cybersecurity) and DoDI 8510.01 (RMF for DoD IT); the DoD publications rely heavily on CNSS and NIST documents
- Other DoD Instructions, DISA STIGs, etc. remain in effect as before

© 2024

44

44

BAI RMF "Publications Library"



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

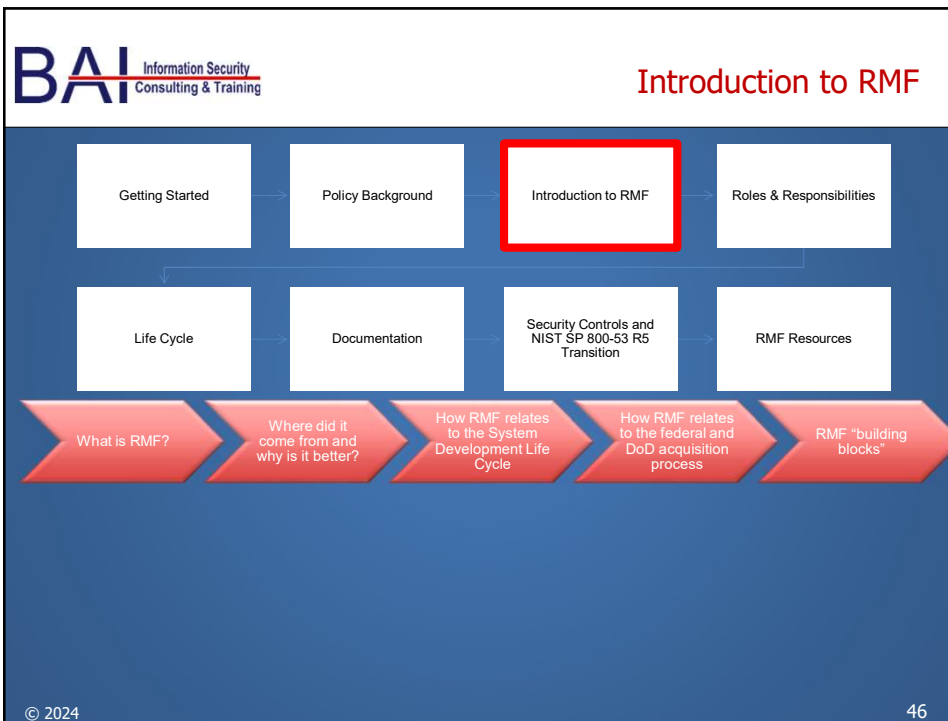
<https://rmf.org/rmf-documents>

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

© 2024

45

45



46

46

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

© 2024 47

47

BAI Who Is the Developer of RMF?

Joint Task Force Transformation Initiative Working Group

NIST Special Publication 800-37
Revision 1

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

Guide for Applying the Risk
Management Framework to
Federal Information Systems
A Security Life Cycle Approach

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

© 2024 48

48

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"

© 2024

49

49

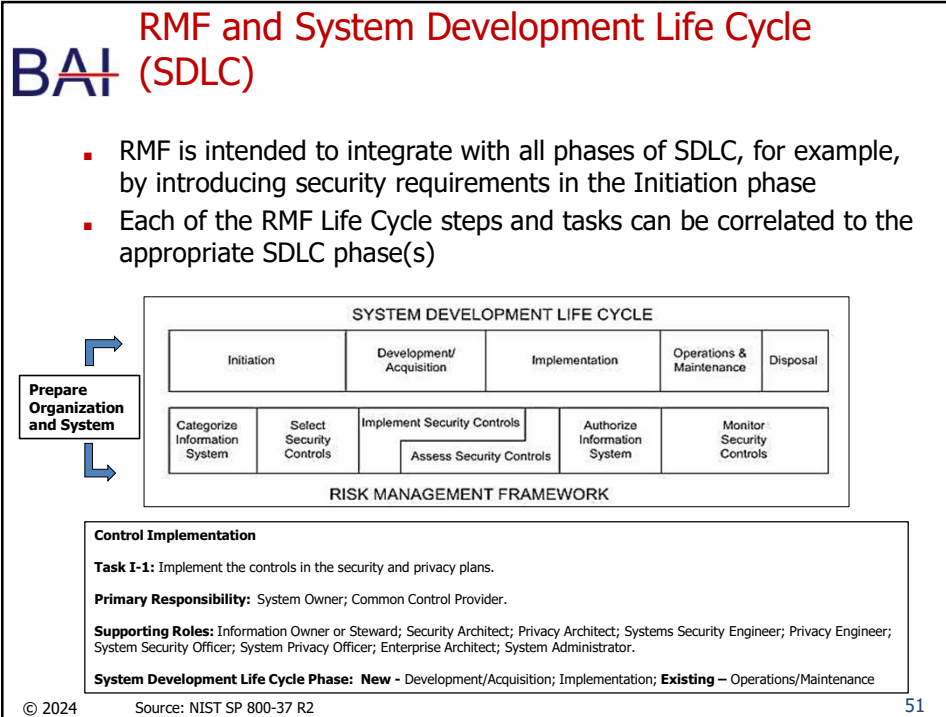
BAI System Development Life Cycle

- 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

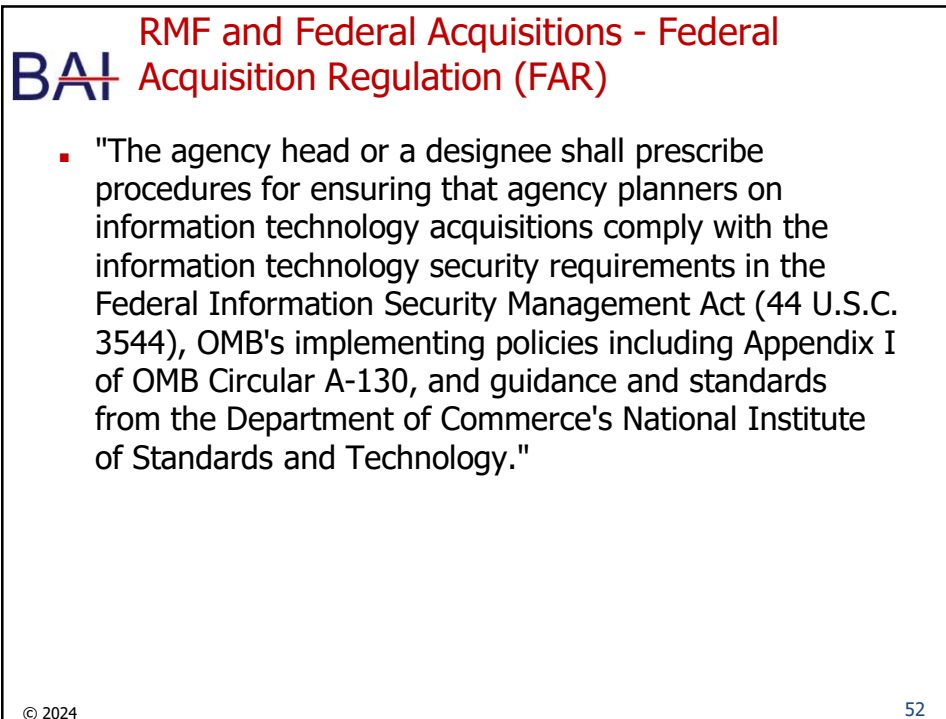
© 2024

50

50



51



52

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

© 2024

53

53

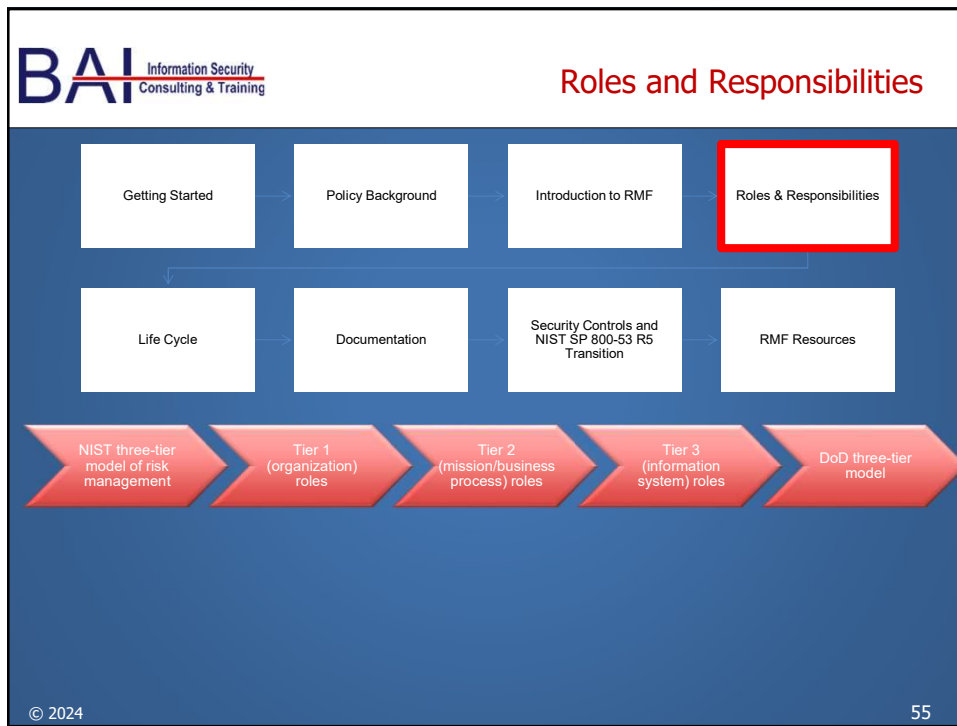
BAI Summary

- 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

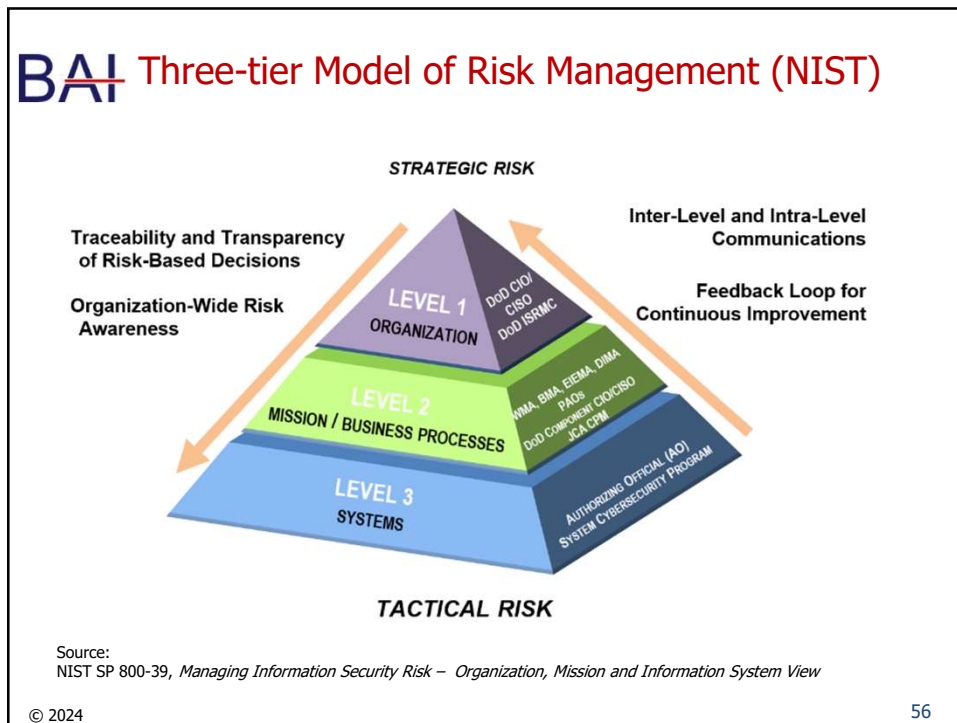
© 2024

54

54



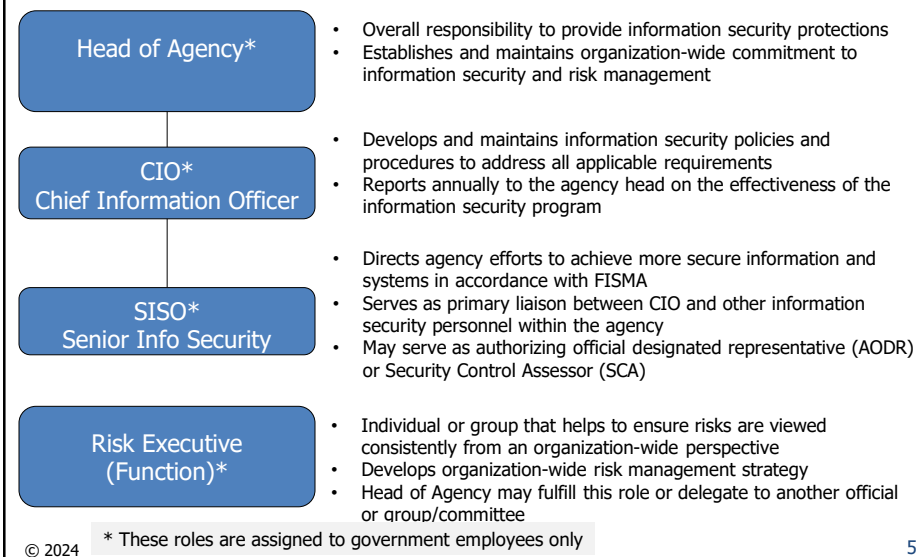
55



56

BAI Top-level RMF Roles (NIST)

Source
NIST SP 800-37 R2

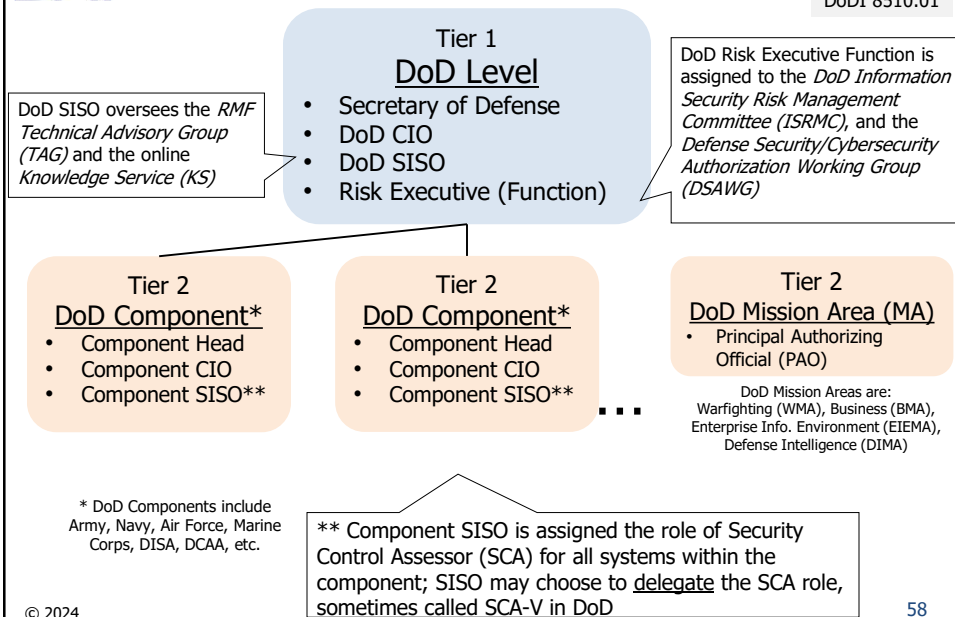


57

57

BAI Top-level RMF Roles (DoD)

Source
DoDI 8510.01



58

58

BAI Role of the Defense Information Systems Agency (DISA)

Technical

- Security Requirements Guides (SRGs)
- Security Technical Implementation Guides (STIGs)
- Control Correlation Identifiers (CCIs)

Enterprise RMF Support Tools

- eMASS

Training

- RMF Training and Awareness Products
- Distributive Learning Environment

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

© 2024 59

59

BAI System-level (Tier 3) Roles (DoD)

- Authorizing Official (AO)
- Information System (IS) or PIT System Cybersecurity Program
 - Information System Owner (ISO)
 - Program Manager / System Manager (PM/SM)
 - User Representative (UR)
 - Information System Security Manager / Officer (ISSM/ISSO)

© 2024 60

60

BAI Authorizing Official (AO)

- Senior-level government employee within business owner and mission owner organization
- Appointed by Component Head
- Responsibilities:
 - Make authorization decisions for IS and PIT Systems within their purview
 - Ensure RMF tasks are completed and documented
 - Track POA&Ms
 - Ensure appointees to cybersecurity positions have written statements of responsibilities
- Authorization decisions cannot be delegated; all other responsibilities can be delegated to AO Designated Representative (AODR)

© 2024

61

61

BAI Information System Owner (ISO) and Program/System Manager (PM/SM)

- | | |
|--|--|
| <ul style="list-style-type: none"> ■ ISO (or System Owner) <ul style="list-style-type: none"> ■ Plan and budget for security control implementation, assessment and sustainment ■ Ensure users and support personnel receive cybersecurity training ■ Categorize each assigned system ■ Appoint a User Representative (UR) ■ Develop, maintain and track the Security Plan (SP) | <ul style="list-style-type: none"> ■ PM/SM <ul style="list-style-type: none"> ■ Register the system per DoD Component procedures ■ Appoint an ISSM for each assigned system ■ Ensure each system has an assigned security engineer ■ Develop a system description ■ Implement RMF ■ Ensure RMF activities are aligned with acquisition process ■ Enforce AO authorization decision ■ Develop and track a POA&M for each system |
|--|--|

In many organizations, ISO and PM/SM roles are assigned to the same individual

© 2024

62

62

BAI User Representative (UR)

- Represent the operational interests of the user community in the RMF process

NOTE: The UR role is retained from DIACAP; a specific UR role does not appear in the NIST RMF publications

© 2024

63

63

BAI Information System Security Manager/Officer (ISSM/ISSO)

- | | |
|--|--|
| <ul style="list-style-type: none"> ■ ISSM (formerly IAM)* <ul style="list-style-type: none"> ■ Develop/maintain organizational cybersecurity program (architecture, requirements, policies, procedures, personnel) ■ Ensure information owners / stewards are identified ■ Appoint and oversee ISSOs ■ Maintain a repository for cybersecurity documentation ■ Monitor compliance with security policy ■ Act as cybersecurity technical advisor ■ Respond to cybersecurity incidents and spillage | <ul style="list-style-type: none"> ■ ISSO (formerly IAO)* <ul style="list-style-type: none"> ■ Assist ISSM ■ Enforce cybersecurity policies and procedures ■ Ensure users have appropriate clearances and authorization before access is granted ■ Ensure cybersecurity documentation is up-to-date and accessible to authorized individuals |
|--|--|

*In smaller DoD organizations, the same individual may assume both ISSM and ISSO roles

NOTE: NIST RMF publications assign all these responsibilities to "ISSO"

© 2024

64

64

BAI Additional Roles

- Information Owner / Steward (IO)
- Common Control Provider
- Information Security Engineer
- Information Security Architect

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

© 2024

65

65

BAI Information Owner/Steward (IO)

- Official with statutory, management or operational authority for specified information
- Responsible for establishing policies and procedures for its generation, collection, processing, dissemination and disposal
- May or may not be the Information System Owner
- A single system may contain information from multiple IOs

© 2024

66

66

BAI Common Control Provider

- Responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).

© 2024

67

67

BAI Information Security Architect (ISA) Information System Security Engineer (ISSE)

Information Security Architect (ISA)

- Ensures security requirements are integrated into enterprise architecture

Information System Security Engineer (ISSE)

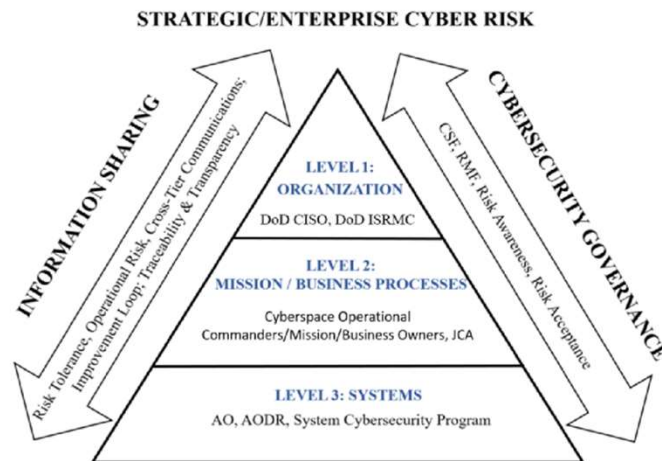
- Ensures security requirements are integrated into information system and product acquisition, design and configuration

© 2024

68

68

BAI Three-Tier Model (DoD)



Sources:
DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*

© 2024

69

69

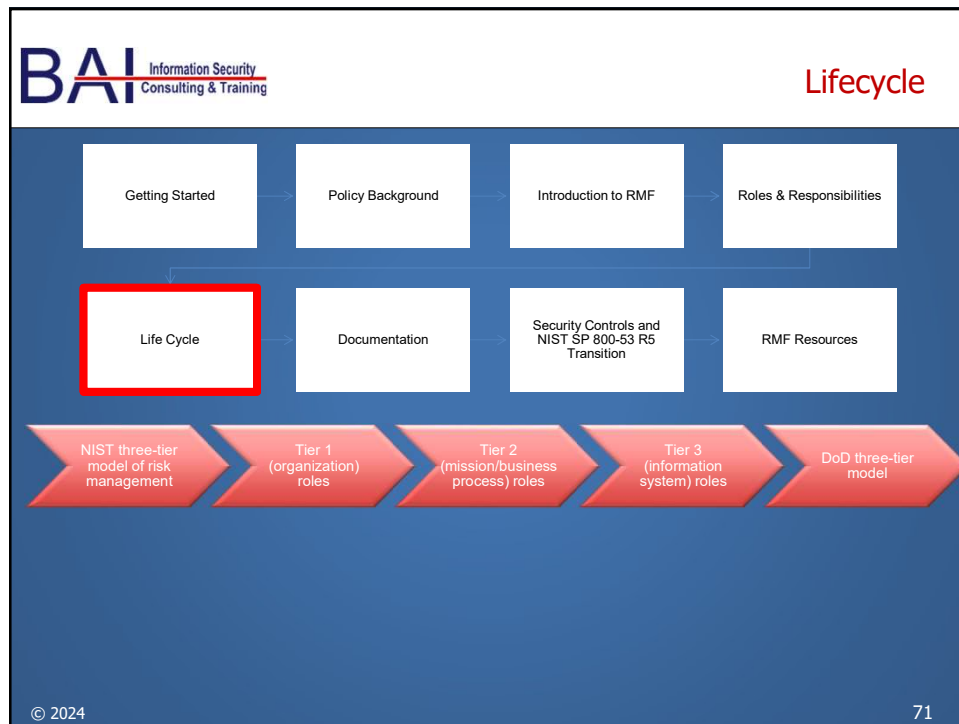
BAI Summary

- NIST defines a three-tier model for risk management
 - Tier 1 – Organization
 - Tier 2 – Mission/Business Process
 - Tier 3 – Information Systems
- DoD adoption/adaptation of the three-tier model
 - Tier 1 – DoD Enterprise
 - Tier 2 – DoD Component CIO/SISOs and Mission Area PAOs
 - Tier 3 – DoD IS and PIT Systems
- Tier 1 and 2 roles include Agency Head, CIO, SISO, Risk Executive (function)
- Tier 3 roles include AO, ISO, PM/SM, UR, ISSM/ISSO
- Additional roles include IO, Common Control Provider, ISA, ISSE

© 2024

70

70



71

BAI Two Types of IT Systems
(Per OMB and NIST Publications)

General Support System (GSS)

- "Interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people."
- Examples of GSS are data centers and communication networks.

Major Application (MA)

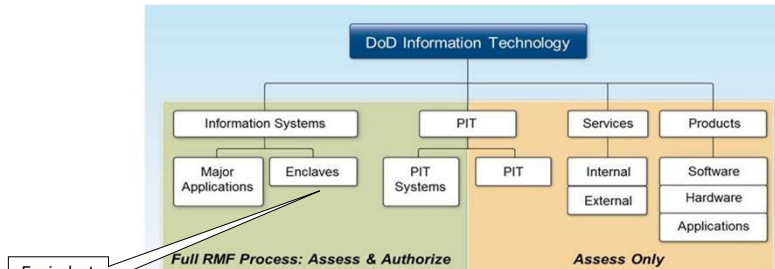
- "An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application."
- MAs typically rely on a GSS for some (but not all) of their security protection.

© 2024 72

72

BAI DoD Information Technology

Source: DoDI 8500.01



Equivalent of GSS

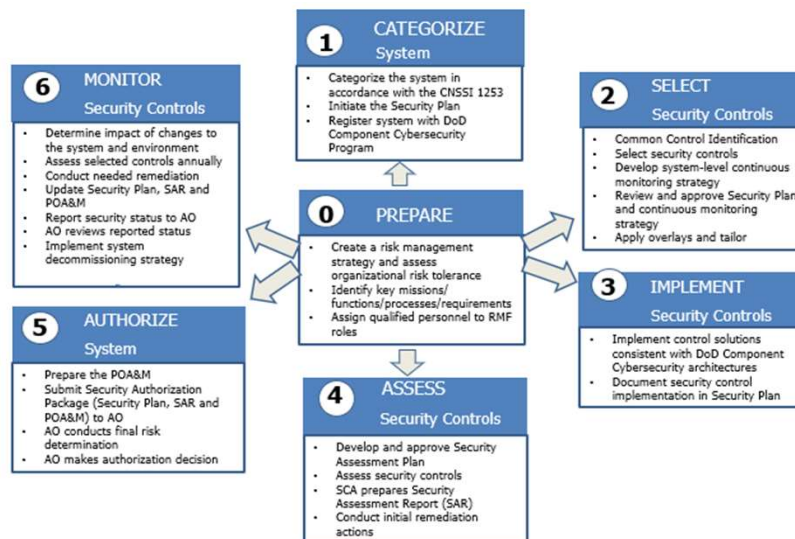
- Major Applications, Enclaves and PIT Systems are assessed and authorized (full RMF life cycle) before being placed into operation
- Other IT Types (PIT, Services, Products) are assessed for compliance before being added to an already authorized system

© 2024

73

73

BAI DoD RMF Life Cycle



Source: DoD Knowledge Service

© 2024

74

74

BAI DoD RMF Prerequisites (Aligns with NIST "Preparation" step)

- 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)
 - ISSM/ISSO
 - Information Owner(s)
 - Assign other key resources
- Know the requirements
 - Which DoD component cybersecurity program?
 - "Unique" security requirements
 - Formal or informal risk assessment

© 2024

75

75

BAI Assign Qualified Personnel to RMF Roles

- RMF Team normally includes:
 - System Owner (and/or PM/SM)
 - Information Owner (if different)
 - ISSM/ISSO
 - UR
 - AO (or Designated Representative)
 - SCA (or Designated Representative)
- Avoid conflict of interest when assembling the RMF team
- Record RMF team member names and contact information in the SP

© 2024

76

76

BAI NIST SP 800-37 R2 (RMF 2.0)

- Preparation – Organization requirements (Notice Cybersecurity Framework linkages – more on CSF in upcoming slide)

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]

© 2024

77

77

BAI 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]

©

78



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



© 2024

<https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters>

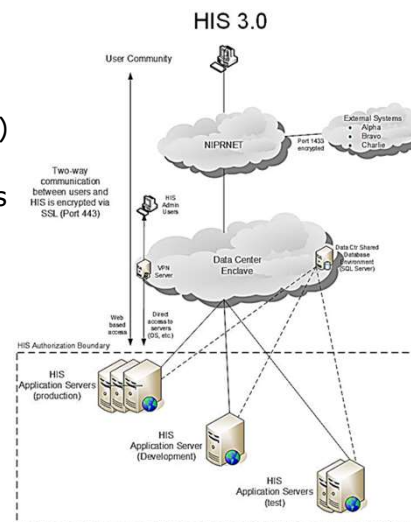
79

79



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



© 2024

80

80

BAI Step 1 – Categorize Activities



Categorize the System in
Accordance with CNSSI 1253



Initiate the Security Plan



Register System with Component
Cybersecurity Program

© 2024

Source: DoD Knowledge Service 81

81

BAI Categorize the System in Accordance with CNSSI 1253 (NSS and DoD)

- Systems are categorized as High, Moderate or Low for each of the three security objectives (C-I-A)
- 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:
Confidentiality: LOW
Integrity: HIGH
Availability: HIGH

© 2024

82

82

BAI NIST SP 800-60 (Rev 1)

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**.

© 2024

83

83

BAI System Categorization (DIACAP vs. RMF)

MAC	CL
I	Classified
I	Sensitive
I	Public
II	Classified
II	Sensitive
II	Public
III	Classified
III	Sensitive
III	Public

DIACAP

RMF

Confidentiality	Integrity	Availability
High	High	High
High	High	Moderate
High	High	Low
High	Moderate	High
High	Moderate	Moderate
High	Moderate	Low
High	Low	High
High	Low	Moderate
High	Low	Low
Moderate	High	High
Moderate	High	Moderate
Moderate	High	Low
Moderate	Moderate	High
Moderate	Moderate	Moderate
Moderate	Moderate	Low
Moderate	Low	High
Moderate	Low	Moderate
Moderate	Low	Low
Low	High	High
Low	High	Moderate
Low	High	Low
Low	Moderate	High
Low	Moderate	Moderate
Low	Moderate	Low
Low	Low	High
Low	Low	Moderate
Low	Low	Low

© 2024

84

BAI Sidebar: System Categorization of non-NSS (outside of DoD)

- For categorization of non-NSS outside DoD, agencies can also use FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- The process is almost identical - for highest categorization level among the three security objectives
- If the system on the previous slide were a non-NSS outside of DoD, it would be categorized as HIGH

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

→ System Categorization is: HIGH

© 2024 85

85

BAI Initiate the Security Plan

- 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 like eMASS

© 2024 86

86

BAI Register System with DoD Component Cybersecurity Program

- Each DoD Component has its own process for system registration, which may entail one or both of the following
 - Registration in a Component-level or DoD-level "IT Registry"
 - Registration with the Component SISO or cybersecurity management office
- Systems typically receive a registration number that should be recorded in the SP

© 2024 87

87

BAI Step 2 – Select Activities

Select Security Controls

Common Control Identification

Apply Overlays and Tailor

Develop System-level Continuous Monitoring Strategy

Review and Approve the Security Plan and Continuous Monitoring Strategy

© 2024 Source: DoD Knowledge Service

88

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)

© 2024

89

89

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

Note the use of organization-defined values

c. Coordinate results of reviews and investigations with the organizational incident response capability.

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](#).

© 2024

Source: NIST SP 800-53 R5

90

90

BAI Security Control Example (cont.)

Control enhancements are best thought of as simply additional controls.

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.

Source: NIST SP 800-53 R5

© 2024

91

91

BAI Organization-defined Values for NSS and DoD

PE-6 MONITORING PHYSICAL ACCESS

b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events];

Note the use of organization-defined values

Organization-defined values (CNSSI 1253, Appendix E, 27 Mar 2014)

ID	Control Text	Defined Value for NSS
PE-6	b. [Assignment: organization-defined frequency] [Assignment: organization-defined events or potential indications of events]	b. At least every 90 days if not otherwise defined in formal organizational policy. Not appropriate to define at the CNSS level for all NSS.

CHANGE: Organization-defined values (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							
				L	M	H	L	M	H	L	M	H			Assurance	Resiliency	ATT&CK
PE-6	Monitoring Physical Access		√ _{2.3}	X	X	X	X	X	X	X	X	X		b. 1st PV: at least every 90 days	√	√	

© 2024

92

92

BAI Security Control Selection for NSS and DoD

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				√	√

If the organization determines it must employ one of the controls designated as having a privacy implementation consideration, the Senior Agency Official for Privacy (SAOP) or designee must be consulted to determine if additional steps are required to protect privacy. Subscripted numbers in this column are described on pg. D-1 for considering when implementing control.

- 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.

© 2024

93

93

BAI Security Control Example

Source
RMF Knowledge
Service

Control Number	Control Title	Control Text	Supplemental Guidance
PE-6	MONITORING PHYSICAL ACCESS	The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.	Supplemental Guidance: Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.
PE-6(1)	MONITORING PHYSICAL ACCESS INTRUSION ALARMS / SURVEILLANCE EQUIPMENT	The organization monitors physical intrusion alarms and surveillance equipment.	
PE-6(2)	MONITORING PHYSICAL ACCESS AUTOMATED INTRUSION RECOGNITION / RESPONSES	The organization employs automated mechanisms to recognize [Assignment: organization-defined classes/types of intrusions] and initiate [Assignment: organization-defined response actions].	Supplemental Guidance: Related control: SI-4.
PE-6(3)	MONITORING PHYSICAL ACCESS VIDEO SURVEILLANCE	The organization employs video surveillance of [Assignment: organization-defined operational areas] and retains video recordings for [Assignment: organization-defined time period].	Supplemental Guidance: This control enhancement focuses on recording surveillance video for purposes of subsequent review, if circumstances so warrant (e.g., a break-in detected by other means). It does not require monitoring surveillance video although organizations may choose to do so. Note that there may be legal considerations when performing and retaining

The Knowledge Service is projected to update this information to reflect NIST SP 800-53 R5 in early 2024.

© 2024

94

94

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

© 2024

95

95

BAI Apply Overlays and Tailor

- 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”
 - Supplementing the baseline with controls to address “unique” security requirements
 - The Security Plan should be revised to reflect the tailored baseline (including appropriate justification)

© 2024

96

96

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
- Overlays currently available on the CNSS website:
 - Classified systems
 - Privacy (PII, HIPAA)
 - Space systems
 - Intelligence systems
 - Cross-domain solutions
- Additional Overlays available:
 - Operational Technology (Industrial Control) Systems (NIST SP 800-82)
 - DoD Financial Management (FM) Overlay (Knowledge Service)

NOTE
CNSSI 1253 Appendix F1
contains a template for
overlay development

© 2024

97

97

BAI 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 the federal reference on this subject
- Knowledge Service provides DoD summary of Continuous monitoring

© 2024

98

98

BAI 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 DoD Component may have its own process for submitting the SP for AO approval

© 2024 99

99

BAI Step 3 – Implement Activities

 Implement control solutions consistent with DoD component cybersecurity architectures

 Document security control implementation in the security plan

Source: DoD Knowledge Service

© 2024 100

100

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., DISA Security Technical Implementation Guides (STIGs))

© 2024

101

101

BAI Self-Assessment – Verification of Control Implementation

- Self-Assessment is mandated for DoD security controls
- DoD self-assessment is conducted via Control Correlation Identifiers (CCIs), “assessment objectives” which can be found on the DISA website, DoD Knowledge Service and automated tools (i.e., eMASS)

© 2024

102

102

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


© 2024 103

103


BAI Step 4 – Assess Activities




Develop and Approve Security Assessment Plan



Assess Security Controls



SCA Prepares Security Assessment Report (SAR)



Conduct Initial Remediation Actions

© 2024 Source: DoD Knowledge Service 104

104

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 R5, RMF Knowledge Service (KS)
- Prepared by the Security Control Assessor (SCA)*
- Reviewed/approved by: AO

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

© 2024

105

105

BAI 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].

© 2024

Source: NIST SP 800-53A R5

106

106

BAI Assessment Procedure Example

Source: RMF KS

CCI	Control ID	800-53 Control Text Indicator	CCI Definition	Assessment Procedures
CCI-002939	PE-6	PE-6 (a)	The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.	The organization conducting the inspection/assessment obtains and examines the inspected organization's monitoring procedures addressing physical access monitoring. Organizational personnel with physical access monitoring responsibilities are to be interviewed. The objective of the reviews and interviews is to validate the organization is actively monitoring its physical access intrusion alarms and surveillance equipment to detect and respond to all physical access security incidents.
CCI-000940	PE-6	PE-6 (b)	The organization defines a frequency for reviewing physical access logs.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 30 days.
CCI-000939	PE-6	PE-6 (b)	The organization reviews physical access logs in accordance with organization-defined frequency.	The organization conducting the inspection/assessment obtains and examines the inspected organization's physical access logs or records; physical access incident reports; and any other relevant documents or records. The purpose of the reviews is to determine if the organization is conducting reviews of the physical access logs every 30 days. DoD has defined the frequency as every 30 days.

CCI = Control Correlation Identifier

Organization-defined

The Knowledge Service is projected to update this information to reflect NIST SP 800-53A R5 in early 2024.
© 2024 107

107

BAI Assess Security Controls in DoD

- A Security Control Assessment is conducted which includes:
 - Executing assessment procedures as documented in NIST SP 800-53A R5 and the RMF Knowledge Service (KS)
 - Assessing IT products for compliance with STIGs and SRGs as required
 - Verifying inherited controls with Common Control Providers
- Each control assessment procedure (i.e., CCI for DoD) in the approved baseline is assessed as Compliant (C), Non-compliant (NC), or Not Applicable (NA)
- Assessment activities may be conducted on-site, remotely, or a combination of both

© 2024

108

108



SCA Prepares Security Assessment Report (SAR)

- SAR content for each control
 - Description of assessment procedure and result
- SAR content for each NC control
 - Supporting data showing which portion(s) of the control were not compliant and why
 - Vulnerability Severity Value* (VL-very low, L-low, M-moderate, H-high, VH-very high)
 - Risk Level* (VL, L, M, H, VH)
 - Recommended mitigation
- Assessment of overall (aggregate) system risk
- Additional information/recommendations

* Vulnerability Severity Value considers only the assessment finding itself, whereas the Risk Level also considers external mitigating factors along with likelihood and impact.

© 2024

109

109



Conduct Initial Remediation Actions

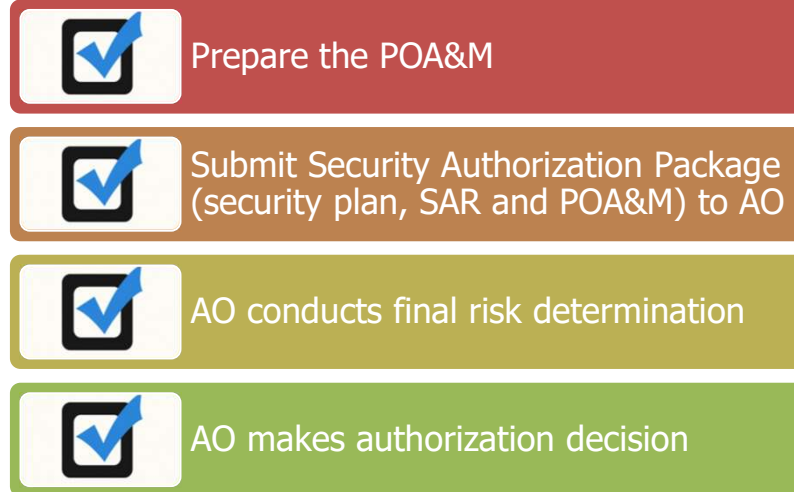
- Having received the SAR, the System Owner may choose to address some or all the NC controls “immediately” and request reassessment
- Reassessed controls should be so noted in the SAR
- SAR feeds the Risk Assessment Report (RAR) which is maintained throughout the life cycle of the system

© 2024

110

110

BAI Step 5 – Authorize Activities



© 2024

Source: DoD Knowledge Service

111

111

BAI Prepare the POA&M

- System Owner or PM/SM 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
 - Component SISO

© 2024

112

112

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 ISSM and sent to the AO (or via the AODR) for review and approval

© 2024

113

113

BAI AO Makes Authorization Decision

- Basis of authorization decision
 - Are there any NC controls with risk level of Very High (VH) or High (H)?
 - Is the overall system risk acceptable?
- Potential authorization decisions
 - Authorization to Operate (ATO)
 - ATO with Conditions (replaces DIACAP IATO)
 - Denial of Authorization to Operate (DATO)
 - Interim Authorization to Test (IATT)

© 2024

114

114

BAI Authorization Decisions

- ATO
 - AO must specify an Authorization Terminate Date (ATD) of 3 years or less
 - Continuous monitoring ➡ "Ongoing authorization"
- ATO with Conditions
 - AO must specify a "review" within 6 months
 - If there are still VH or H controls after one year, Component CIO must grant permission to continue
- DATO
 - If system is currently operational, it must be disconnected
- IATT
 - Should only be sought if specific functional testing activities require connection to a "live" network
 - Typically issued for the duration of testing activity (normally 90 days or less)

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

© 2024

115

115

BAI Type Authorization

- Used to deploy identical copies of an IS or PIT system 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

© 2024

116

116

BAI Reciprocity





- 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
 - If risk is acceptable, executes an agreement (MOA, MOU, SLA) with the deploying organization for ongoing maintenance and monitoring of the security posture of the system
 - Documents acceptance by the receiving AO
 - Updates its authorization to show inclusion of the deployed system

© 2024

117

117

BAI Step 6 – Monitor Activities

-  Determine impact of changes to the system and environment
-  Assess selected controls annually
Conduct needed remediation
Update security plan, RAR and POA&M
-  Report security status to AO
AO reviews reported status
-  Implement system decommissioning strategy

© 2024

Source: DoD Knowledge Service

118

118

BAI Maintaining Security Posture Over Time

- Effective change management is essential
- Show current changes:
 - Performance monitoring
 - Periodic independent evaluations
- Proposed changes
 - Configuration and change management process

© 2024

119

119

BAI Assess Selected Controls

- Assess a subset of controls in accordance with the approved Continuous Monitoring Strategy
- Assess remainder of controls annually per FISMA
- Update RAR and POA&M
- Assessor reports to AO
- AO reviews

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

© 2024

120

120

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 ISSM ensure Authorization documents are 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

© 2024

121

121

BAI DoD Enterprise Support of Continuous Monitoring

- Technical solutions
 - Endpoint Security Solutions (ESS) – formerly HBSS
 - Assured Compliance Assessment System (ACAS)
 - Continuous Monitoring and Risk Scoring (CMRS)
- Additional policies and procedures anticipated
- Meanwhile, NIST SP 800-137 is the best-available publication on Continuous Monitoring

NOTE: Even when fully implemented across DoD, these tools support monitoring only technical security elements (e.g., software configuration, vulnerability scanning). System owners will still be responsible for overall monitoring strategy and plan, as well as monitoring of non-technical elements.



© 2024

122

122

BAI Continuous Monitoring and Reassessment

- Per OMB A-130 (Update 2016) systems must:
 - 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
- Continuous Authorization remains a goal for DoD; implementation is dependent on further development and maturity of the continuous monitoring program

© 2024

123

123

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

© 2024

124

124

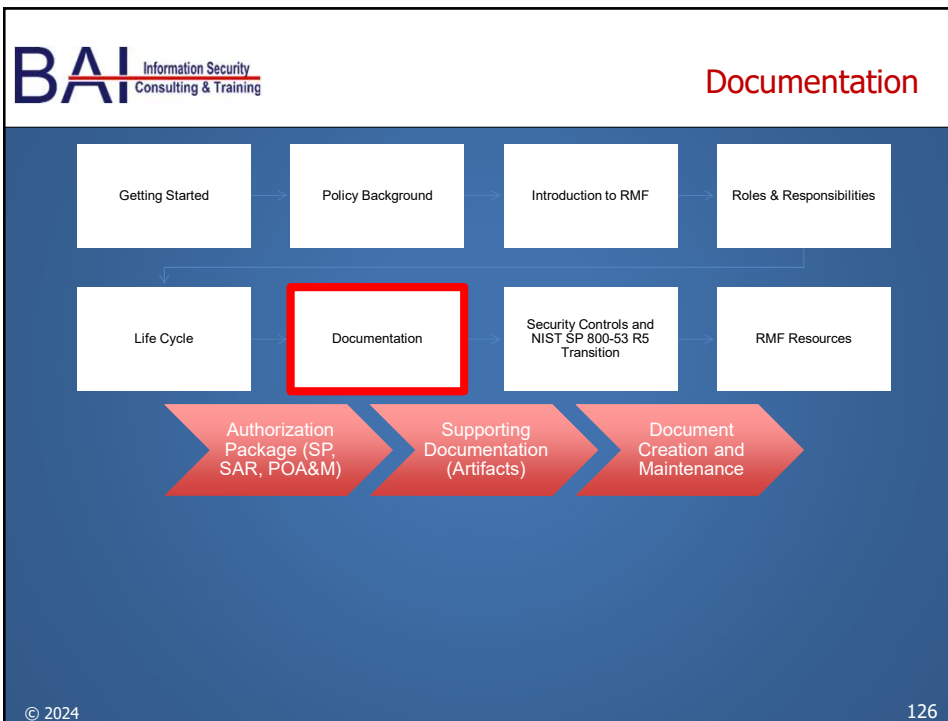
BAI Summary

- DoD IT Enclaves, Major Applications, and PIT 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

© 2024

125

125



126

BAI Authorization Package

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

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 (C, NC, NA)
- For NC controls:
 - Vulnerability severity
 - Risk level
 - Recommended mitigation
- Overall risk level

POA&M Content

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

© 2024

127

127

BAI Artifacts Are Not 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)
- eMASS provides
 - 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 in order to verify control implementation

© 2024

128

128

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
- Automated tool (e.g., eMASS)

© 2024

129

129

BAI eMASS Example – Security Plan (System Information)

Authorization > System Registration > System Overview

System Registration

Step 1 - System Overview

- 1 System Overview
- 2 Authorization Information
- 3 Roles
- 4 Review & Submit

LEGEND

■ Not Yet Started
■ Complete

[i] * Registration Type: Assess and Authorize
 [i] * System Name: eMASS RMF System
 [i] * System Acronym: eMASS RMF System
 [i] * Information System Owner: DOD
 [i] * Version / Release Number: v5.5.2
 [i] * System Type: Platform IT System
 [i] * System Life Cycle / Acquisition Phase: Pre-Milestone A (Material Solution Analysis)
 [i] National Security System: ☒
 [i] Financial Management System: ☒
 [i] Reciprocity System: ☒
 [i] * System Description: Sample system description.
 [i] * DITPR ID: 00000
 [i] DoD IT Registration Number:

Save

Cancel

© 2024

130

130

BAI eMASS Example – Security Plan (Categorization & Control Set)

Primary Security Control Set

Primary Security Control Set: **NIST SP 800-53 Revision 4**

Control Attributes:

- Confidentiality:
- Integrity:
- Availability:

Information Type Evidence: [Browse...](#)

Rationale For Categorization:

Manage Security Controls [Add Additional Controls](#)

Type	Acronym	Name	Control Set	Control Family	Action
A	SC-44	Detonation Chambers	NIST SP 800-53 Revision 4	System and Communications Protection	Delete Comments
B	AC-1	Access Control Policy And Procedures	NIST SP 800-53 Revision 4	Access Control	
B	AC-2	Account Management	NIST SP 800-53 Revision 4	Access Control	
B	AC-2(1)	Automated System Account Management	NIST SP 800-53 Revision 4	Access Control	
B	AC-2(2)	Removal Of Temporary / Emergency Accounts	NIST SP 800-53 Revision 4	Access Control	

© 2024 131

131

BAI eMASS Example (Enter Assessment Results)

Assessment Procedure Details

Assessment Procedure: **AC-2(5).1** [Return to Control: AC-2\(5\)](#)

AP Status: Unassessed Properties: None Control Set Name: NIST SP 800-53 Revision 4 Subject Area Name: Access Control

[Previous: AC-2\(4\).11](#) [AC-2\(5\).1](#) [Go](#) [Next: AC-2\(5\).2](#)

AP Information [Collapse](#)

Description [Collapse](#)

OC # 002153

OC Definition: The organization defines other conditions when users are required to log out.

Procedure: The organization conducting the inspector/assessment outlines and examines the documented conditions to ensure they have been defined. DOD has determined the conditions are not appropriate to define at the Enterprise level.

Implementation Guidance: The organization being inspected/assessed defines and documents the other conditions when users are required to log out, you first determines the conditions are not appropriate to define at the Enterprise level.

Recommended Longevity Indicator: 1) Sign-in and control documentation that all defines the other original/undefined condition requirements for logging out.

Inheritance [Collapse](#)

Add Test Results

Status:

Test Date:

Tester By:

Test Results:

Save Setting: ☐ Open Save go to Next AP [Save](#) [Cancel](#)

© 2024 132

132

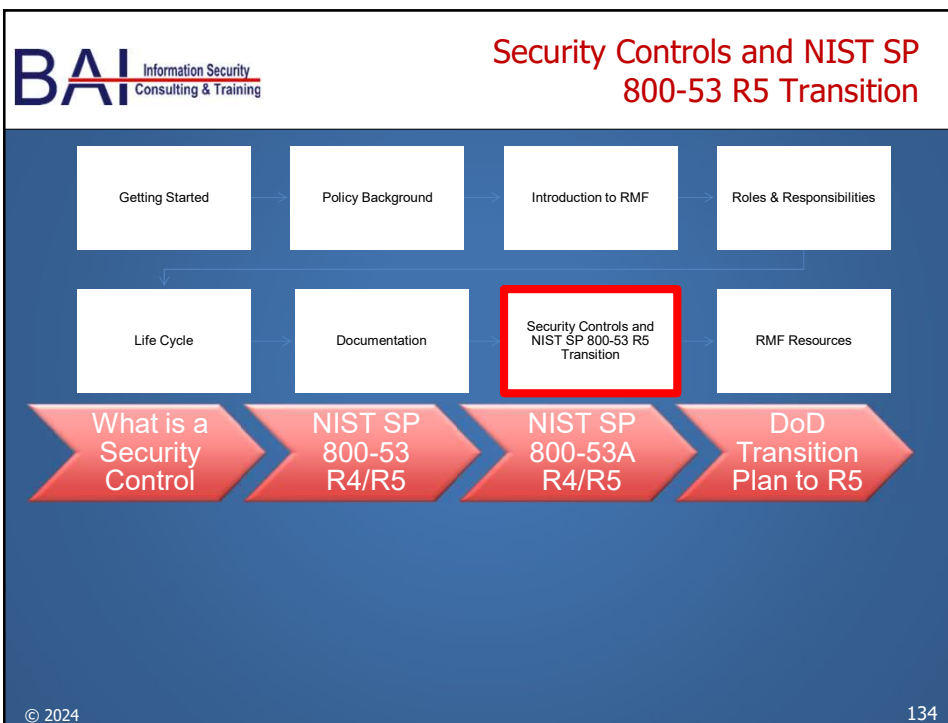
BAI Summary

- 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, Excel, PDF documents; organizational templates
 - Automated tool such as eMASS
 - Accessibility, version control, information sensitivity and document marking need to be considered

© 2024

133

133



134

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”

© 2024

135

135

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

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

© 2024

JOINT TASK FORCE

136

136

BAI NIST SP 800-53 R5 – Published September 2020

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)

© 2024

137

137

BAI 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)	REVOCATION
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

© 2024

138

138

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

© 2024

139

139

BAI 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

© 2024

140

140

BAI NIST SP 800-53 R5

- 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 and DoD will continue to use CNSSI 1253.)

© 2024

* A rapidly broadening landscape of connected devices, known as the Internet of Things (IoT).

141

141

BAI Example Control from Rev 5

Control ID and Title

Control Text

Discussion

Control Enhancements

- Number
- Title
- Text
- Supplemental
- Guidance

Reference

No Baseline

Moved to SP 800-

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].

© 2024

142

142

BAI Assessment Procedures – Now NIST SP 800-53A R5

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>

© 2024 143

143


BAI Assessment Procedure Example

NIST SP 800-53A

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].

© 2024 144

144



Assessment Procedure Example


RMF KS

CCI	Control ID	Control Test	CCI Definition	Implementation Guidance	Assessment Procedures
CCI-000818	IR-3	IR-3	The organization tests the incident response capability for the information system on an organization-defined frequency using organization-defined tests to determine the incident response effectiveness.	<p>The organization being inspected/assessed documents and implements a process to test its incident response capability for the information system at least every six months for high availability and at least annually for low/med availability using tests and as defined in the incident response plan.</p> <p>The organization must maintain a record of test results.</p> <p>DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability.</p> <p>DoD has defined the tests as tests as defined in the incident response plan.</p>	<p>The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of test results to ensure the organization being inspected/assessed tests its incident response capability for the information system at least every six months for high availability and at least annually for low/med availability using tests and as defined in the incident response plan.</p> <p>DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability.</p> <p>DoD has defined the tests as tests as defined in the incident response plan.</p>
CCI-000819	IR-3	IR-3	The organization defines a frequency for incident response tests.	DoD has defined the frequency as at least every six months for high availability and at least annually for low/med availability.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.
CCI-000820	IR-3	IR-3	The organization defines tests for incident response.	DoD has defined the tests as tests as defined in the incident response plan.	The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.
CCI-001624	IR-3	IR-3	The organization documents the results of incident response tests.	The organization being inspected/assessed will document the results of incident response tests.	<p>The organization conducting the inspection/assessment obtains and examines:</p> <ol style="list-style-type: none"> the organization's incident response plan to identify organization's testing schedule and, results of previous incident response tests to ensure the organization is documenting the results IAW their incident response plan.
CCI-000821	IR-3(I)	IR-3(I)	The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.	The organization being inspected/assessed will identify and employ automated mechanisms to test the incident response capability for the information system.	The organization conducting the inspection/assessment obtains and examines the identified automated mechanisms in use to test the incident response capability for the information system.

The Knowledge Service is projected to update this information to reflect NIST SP 800-53A R5 in early 2024.

© 2024
145

145



DoD Transition Plan to NIST SP 800-53 R5

- DoD Phased Adoption of 800-53 Rev. 5

- Formal Adoption Recommendation of 800-53 Rev 5
 - eMASS Updates
 - RMF Knowledge Service Site Updates

October 2023

January 2024

January 2024

- DoD currently plans to transition systems from Rev 4 to Rev 5 controls in a phased approach, in conjunction with regular system ATO reviews.

System Authorization Status Transition Timeline And Instructions

New start or unaccredited operational system

Begin transition to new version of CNSSI 1253 within 6 months of DoD adoption.

© 2024

Source: Knowledge Service

146

146



DoD Transition Plan to NIST SP 800-53 R5 (continued)

System has initiated RMF, but has not yet begun executing the security plan	Begin transition to new version of CNSSI 1253 within 6 months of DoD adoption.
System is executing the RMF security plan	Either: a. Continue under the current version of CNSSI 1253. Develop a strategy and schedule for transitioning to the new version of CNSSI 1253. Obtain AO's approval of the strategy and schedule. The schedule for transitioning must not exceed the system re-authorization timeline. Or; b. Begin transition to the new version of CNSSI 1253.
System has a RMF system authorization decision that is current within 3 years	Develop a strategy and schedule for transitioning to the new version of CNSSI 1253. Obtain AO's approval of the strategy and schedule. The schedule for transitioning must not exceed the system re-authorization timeline.
System has an RMF system authorization that is more than 3 years old	Begin transition to the new version of CNSSI 1253 immediately

© 2024

147

147



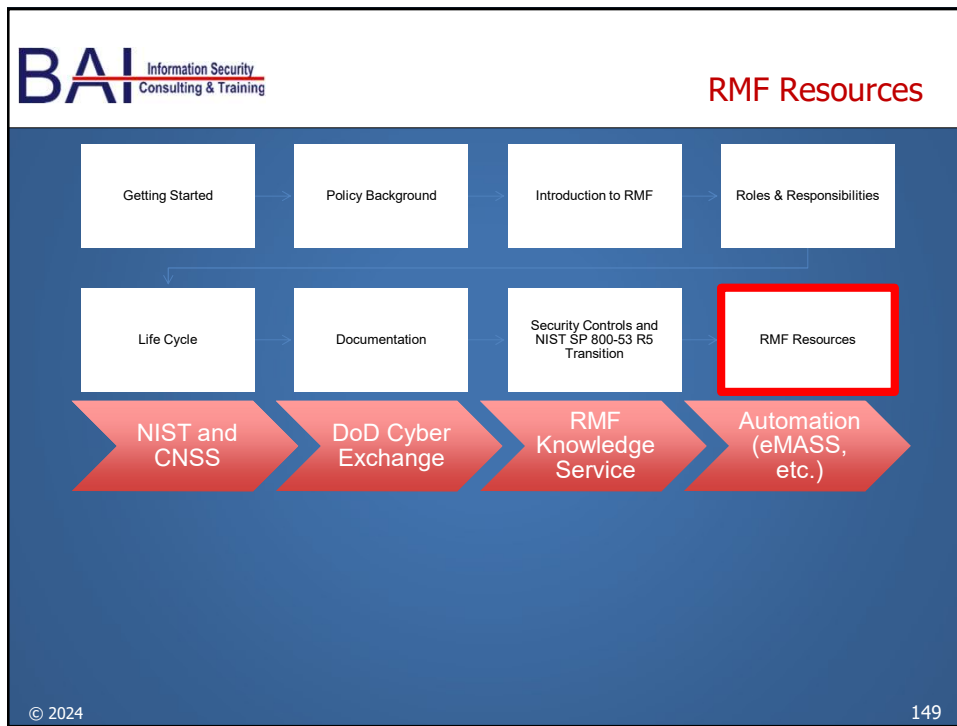
Summary

- Security control is a concise statement of a specific safeguard/countermeasure
- NIST SP 800-53 R4/R5 contains the "catalog" of security controls used by RMF for DoD IT
- For all DoD systems (and NSS outside of DoD), security control baseline is selected in accordance with CNSSI 1253 (non-NSS in Federal Agencies use FIPS 200 and NIST SP 800-53B for security control baseline)
- NIST SP 800-53A R4/R5 contains a "catalog" of assessment objectives and methods for each of the controls and control enhancements
- DoD Control Correlation Identifiers (CCIs) are assigned to each assessment objective
- DoD Transition Plan to NIST SP 800-53 R5 is now published on the Knowledge Service

© 2024

148

148



149

BAI NIST CSRC

NIST Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

Search CSRC 🔍 CSRC MENU

- Projects
- Publications
- Topics
- News & Updates
- Events
- Glossary
- About CSRC

CHECK OUT NIST'S NEW "CYBERSECURITY INSIGHTS" BLOG

USABLE CYBERSECURITY RESEARCH AT NIST

OCTOBER IS "NATIONAL CYBER SECURITY AWARENESS MONTH." LEARN ABOUT NIST'S ACTIVITIES!

For 20 years, the **Computer Security Resource Center (CSRC)** has provided access to NIST's cybersecurity- and information security-related **projects, publications, news** and **events**. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

Source: <https://csrc.nist.gov>

© 2024 150

150

BAI NIST CSRC – Publications Page

NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER **CSRC**

Search CSRC: **CSRC MENU**

Projects

Publications

Drafts for Public Comment

NIST Special Publications (SPs)

FIPS

NIST Internal/Interagency Reports (NISTIRs)

ITL Bulletins

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)

Topics **NISTIR** **NIST Internal or Interagency Reports** Reports of research findings, including background information

© 2024 151

151

BAI NIST CSRC – Subscribe for Updates

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

Want updates about CSRC and our publications? **Subscribe**

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

PROJECTS

PUBLICATIONS

Draft Pubs

Final Pubs

FIPS

Special Publications (SPs)

NISTIRs

ITL Bulletins

White Papers

Journal Articles

Conference Papers

Books

TOPICS

Security & Privacy

Applications

Technologies

Sectors

Laws & Regulations

Activities & Products

NEWS & UPDATES

EVENTS

GLOSSARY

ABOUT CSRC

Computer Security Division

Applied Cybersecurity Division

Contact Us

Information Technology Laboratory (ITL)

Computer Security Division (CSD)
TEL: 301.975.8443

Applied Cybersecurity Division (ACD)

Contact CSRC Webmaster:
webmaster-csrc@nist.gov

Email Updates
To sign up for updates or to access your subscriber preferences, please enter your contact information below.

Subscription Type

Email Address

SUBMIT **CANCEL**

Your contact information is used to deliver requested updates or to access your subscriber preferences.

© 2024 Privacy Policy - Help 152

Recommended!

152

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) ⓘ
 - ☒ Federal Information Processing Standards (FIPS) ⓘ
 - ☒ Special Publications (SPs) ⓘ
 - ☒ NIST Interagency Reports (NISTIRs) ⓘ
 - ☒ ITL Security Bulletins ⓘ
 - ☒ Announcements ⓘ
 - ☒ NIST Cybersecurity Events ⓘ

☐ Federal Information Security Management Act (FISMA) Project

☐ Trusted Identities Group (TIG)

☐ Federal Information Security Management Act (FISMA) Project

☐ Trusted Identities Group (TIG)

☐ National Initiative for Cybersecurity Education (NICE)

- ☒ NICE ⓘ
- ☒ NICE eNewsletter ⓘ
- ☒ NICE Webinars ⓘ

☒ Cybersecurity Framework

- ☒ Cybersecurity Framework Updates

☐ National Cybersecurity Center of Excellence (NCCoE)

☐ Usable Cybersecurity

© 2024 153

153

BAI CNSS


ABOUT
LIBRARY
HELP
LOGIN
YOUR ACCOUNT
SEARCH 🔍



Committee on
National Security Systems

Meeting Current and Future Threats

<https://www.cnss.gov>

© 2024 154

154

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.

© 2024

155

155

BAI DoD Cyber Exchange (previously DISA IASE)



Topics Training PKI/PKE SRGs/STIGs Resources Help

Welcome to the DoD Cyber Exchange, a new Cyber Experience

The DoD Cyber Exchange is the premier cyber resource for the Department of Defense. Cyber Exchange delivers trusted cyber policies, guidance, cyber security tools and training, and other cyber security resources to the DoD, Federal agencies, and public.

LEARN MORE

VIDEO

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

or

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

© 2024

156

156

BAI DoD Cyber Exchange – STIGs and CCI

DoD CYBER EXCHANGE PUBLIC

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](#)

CCI DOWNLOADS

TITLE	SIZE	UPDATED
CCI List	415.51 KB	01 Aug 2023
CCI List Readme	596 B	30 Mar 2022
CCI Process	37.09 KB	28 Feb 2011
CCI Specification	112.14 KB	01 May 2014

© 2024

157

157

BAI RMF Knowledge Service

RMF KNOWLEDGE SERVICE

(EDIT COMMUNITY LINKS)

RMF Implementation RMF for DoD Technology Controls and Authorization RMF Policy and Governance Collaboration Help and Resources Search this site

Welcome to the Risk Management Framework (RMF) Knowledge Service (KS)

Please use the information below to learn more about the RMF implementation guidance and helpful tools contained within the portal.

RMF Knowledge Service

The Risk Management Framework (RMF) Knowledge Service (KS) is DoD's official site for enterprise RMF policy and implementation guidelines. The RMF Knowledge Service provides Cybersecurity practitioners and managers with a single authorized source for execution and implementation guidance, community forums, and the latest information and developments in the RMF.

Please reference the FAQs page for a list of frequently asked questions on the Risk Management Framework.

<https://rmfks.osd.mil> (CAC or ECA required)

© 2024

158

158

BAI RMF KS Menu Content


RMF Implementation <ul style="list-style-type: none"> Introduction to RMF for DoD IT Prepare Step 1: Categorize System Step 2: Select Security Controls Step 3: Implement Security Controls Step 4: Assess Security Controls Step 5: Authorize System Step 6: Monitor Security Controls RMF Process Assess Only Continuous Authorization to Operate 	RMF for DoD Technology <ul style="list-style-type: none"> Cybersecurity Requirements and Tailoring for DoD Systems and Technology Traditional IT Privacy Role in RMF Control Systems Cybersecurity Trusted Systems and Networks (TSN) and Supply Chain Risk Management (SCRM) Integration of Cybersecurity and Acquisition Cloud Risk Management DoD Mobile Security Automation 	Help and Resources <ul style="list-style-type: none"> Help References Site Changes Log eMASS RMF Training Opportunities Privacy Statement Accessibility Security Notice
Controls and Authorization <ul style="list-style-type: none"> Security Controls Security Authorization Package DoD FM Overlay 	RMF Policy and Governance <ul style="list-style-type: none"> Introduction to RMF Governance Level 1: Organization Level 2: Mission/Business Processes Level 3: Systems RMF Roles Governing Policy Reciprocity Associated Guidance 	Collaboration <ul style="list-style-type: none"> Component Workspaces Discussion RMF TAG RMF TAG Focus Groups RMF TAG Working Groups

© 2024

159

159

BAI RMF KS Content – Selecting Control Baseline


RMF KNOWLEDGE SERVICE

[RMF Implementation](#)
[RMF for DoD Technology](#)
[Controls and Authorization](#)
[RMF Policy and Governance](#)
[Collaboration](#)

RMF KS > Controls and Authorization > Security Controls > [Security Controls Explorer](#)

Security Controls Explorer

The Security Controls Explorer is a tool that has been built for the RMF Knowledge Service to provide an easy way to explore the individual security controls and their families as outlined by the CNSSI 1253. There are two versions of this tool available for use, one being a basic version that presents a streamlined process for choosing confidentiality, integrity, and availability (CIA) selections as well as CNSSI overlays for a particular type of system the user may have in mind. The more advanced version of the tool can be used as a way to browse various controls, their details, and associated assessment procedures utilizing CIA selection filters and overlays just like the base Controls Explorer tool but with the added ability to filter by control family and search terms. Both versions of the tool contain the ability to export customized control sets and implementation guidance and assessment procedure information. For a complete description of the fields within the Security Controls Explorer see the [Introduction to Security Controls](#) page.

[Basic](#)
[Advanced](#)

© 2024

160

160

BAI RMF KS Content – Selecting Control Baseline

Choose Confidentiality	Choose Integrity	Choose Availability
Confidentiality <input type="radio"/> High <input type="radio"/> Moderate <input type="radio"/> Low	Integrity <input type="radio"/> High <input type="radio"/> Moderate <input type="radio"/> Low	Availability <input type="radio"/> High <input type="radio"/> Moderate <input type="radio"/> Low
CNSS Overlays - Please select all that apply		
<input type="checkbox"/> Classified Systems <input type="checkbox"/> Protected Health Information (PHI) <input type="checkbox"/> PII High Confidentiality Impact <input type="checkbox"/> Intelligence-A <input type="checkbox"/> Intelligence-C <input type="checkbox"/> Cross Domain Solution - Transfer	<input type="checkbox"/> PII Moderate Confidentiality Impact <input type="checkbox"/> PII Low Confidentiality Impact <input type="checkbox"/> Space Platform <input type="checkbox"/> Intelligence-B <input type="checkbox"/> Cross Domain Solution - Access <input type="checkbox"/> Cross Domain Solution - Multilevel	
DoD Overlays - Please select all that apply		
<input type="checkbox"/> Nuclear Command and Control, Communications (requires Intelligence-C) <input type="checkbox"/> Financial Management (FM) <input type="checkbox"/> Non-U.S. Persons: 2P Direct Access <input type="checkbox"/> Non-U.S. Persons: 3P Direct Access	<input type="checkbox"/> Facility Related Control Systems (FRCS) <input type="checkbox"/> Non-NSS Systems <input type="checkbox"/> Non-U.S. Persons: 2P Access via Controlled Interface <input type="checkbox"/> Non-U.S. Persons: 3P Access via Controlled Interface	
		<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

© 2024

161

161

BAI RMF KS Content – Security Controls Explorer Advanced

Security Controls Explorer - Advanced Edition

Security Authorization Package Export Beta - After selecting CIA/overlay values, click "Create SAP" to download SAP
Please direct any feedback regarding the new Security Authorization Package to the [Help and Feedback Form](#)

453
 All Control Families

 Choose CIA - Overlay
 Criticality Filter
☐ Red ☐ Yellow ☐ White
 Export

 Security Authorization Package

 Overlay Legend
☐ Altered
☐ Added
☐ Removed

Control Number	Control Title	Criticality	Overlays
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	White	Altered by PII Moderate Confidentiality Impact
AC-2	ACCOUNT MANAGEMENT	Yellow	Altered by PII Moderate Confidentiality Impact
AC-2 (1)	ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT	White	
AC-2 (2)	ACCOUNT MANAGEMENT REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	White	
AC-2 (3)	ACCOUNT MANAGEMENT DISABLE INACTIVE ACCOUNTS	White	
AC-2 (4)	ACCOUNT MANAGEMENT AUTOMATED AUDIT ACTIONS	White	
AC-2 (5)	ACCOUNT MANAGEMENT INACTIVITY LOGOUT	White	
AC-2 (7)	ACCOUNT MANAGEMENT ROLE-BASED SCHEMES	White	
AC-2 (9)	ACCOUNT MANAGEMENT RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS	White	
AC-2 (10)	ACCOUNT MANAGEMENT SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION	Yellow	
AC-2 (12)	ACCOUNT MANAGEMENT ACCOUNT MONITORING / ATYPICAL USAGE	White	
AC-2 (13)	ACCOUNT MANAGEMENT DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	Yellow	Altered by PII Moderate Confidentiality Impact
AC-3	ACCESS ENFORCEMENT	Yellow	Altered by PII Moderate Confidentiality Impact
AC-3 (4)	ACCESS ENFORCEMENT DISCRETIONARY ACCESS CONTROL	White	
AC-3 (9)	ACCESS ENFORCEMENT CONTROLLED RELEASE	White	Added by PII Moderate Confidentiality Impact Altered by PII Moderate Confidentiality Impact
AC-4	INFORMATION FLOW ENFORCEMENT	Yellow	Altered by PII Moderate Confidentiality Impact
AC-4 (15)	INFORMATION FLOW ENFORCEMENT DETECTION OF UNSANCTIONED INFORMATION	White	Added by PII Moderate Confidentiality Impact Altered by PII Moderate Confidentiality Impact

© 2024

162

162

BAI DoD Spreadsheet Example – Security Plan

DoD Security Plan (SP)															
1	System Name:			6	Version/Release #:			11	Authorization Termination Date:			16	Physical Location: Installation or Owning Organization for Type Authorization (including Mobile): Street Address: Building Number: Room Number: City: State: Zip Code: APO/FPO: Country:		
2	System Identification:			7	DoD Component: - Please Select -			12	Governing Mission Area: - Please Select -						
3	Acronym:			8	Ports, Protocols, & Services Management (PPSM) Registry Number:			13	Security Review Date:						
4	System Type: - Please Select -			9	Authorization Status: - Please Select -			14	System Location: Single Location Multiple Location Type Authorization Yes No						
5	System Life Cycle/Acquisition Phase: - Please Select -			10	Authorization Date and Signature:			15	DoD Security Control Set: NIST SP 800-53 Revision 4						
RMF POCs, Member Names, and Contact Information															
17	Title			Name			Phone								
<div> <div>SP</div> <div>SP Instructions</div> <div>SAR</div> <div>SAR Instructions</div> <div>System POA&M</div> <div>POA&M Instructions</div> <div>POA&M (eMASS Template)</div> </div>															

© 2024 163

163

BAI Enterprise Mission Assurance Support System (eMASS)

- “DoD enterprise application, providing workflow, data repository, and documentation assistance for IS Assessment and Authorization”
- Available on both NIPRNET and SIPRNET
- Computer-based training is mandatory to apply for an eMASS account
- eMASS has been adopted on a “component by component” basis over a period of several years
- eMASS instances continue to be built; some now in Federal Agencies

© 2024

164

164

BAI eMASS Content

eMASS Site Agreement

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Access eMASS

eMASS Application Interface:

Home | Welcome to eMASS

Recent Systems List

System	Version	Authorization Status	Last Update
eMASS RMC System	5.6.0	Active	25-May-2020
USCIS RMC System	1.0	Not Yet Authorized	-
DoD Tier III System	1	Expired ATD	31-Mar-2019
DoD Tier III System	1	Not Yet Authorized	-
eMASS Tier III System	1	Expired ATD not Conditions	16-May-2019
USCIS Policy System	1	Unauthorized	-

Workload Tasks

Task Description	System Acronym	Due Date
Create PS&M Item for CP-3.1 in DoD Tier III System	DoD Tier III System	N/A
Create PS&M Item for CP-3.1 in DoD Tier III System	DoD Tier III System	N/A
Create PS&M Item for AR-1.1 in DoD Tier III System	DoD Tier III System	N/A

© 2024

165

165

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/>

© 2024

166

166

BAI Summary

- 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
- DoD Cyber Exchange website is the source of technical configuration guidance (STIGs) as well as RMF information
- RMF Knowledge Service (KS) contains a variety of RMF information, including assessment procedures
- eMASS is DoD's automated solution supporting RMF; commercial automated tools are also available

© 2024

167

167

Summary Learning Objectives Review

- 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, DoD Policy documents)
 - 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 for DoD IT

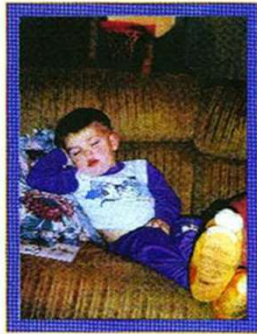
© 2024

168

168

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

© 2024

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

169