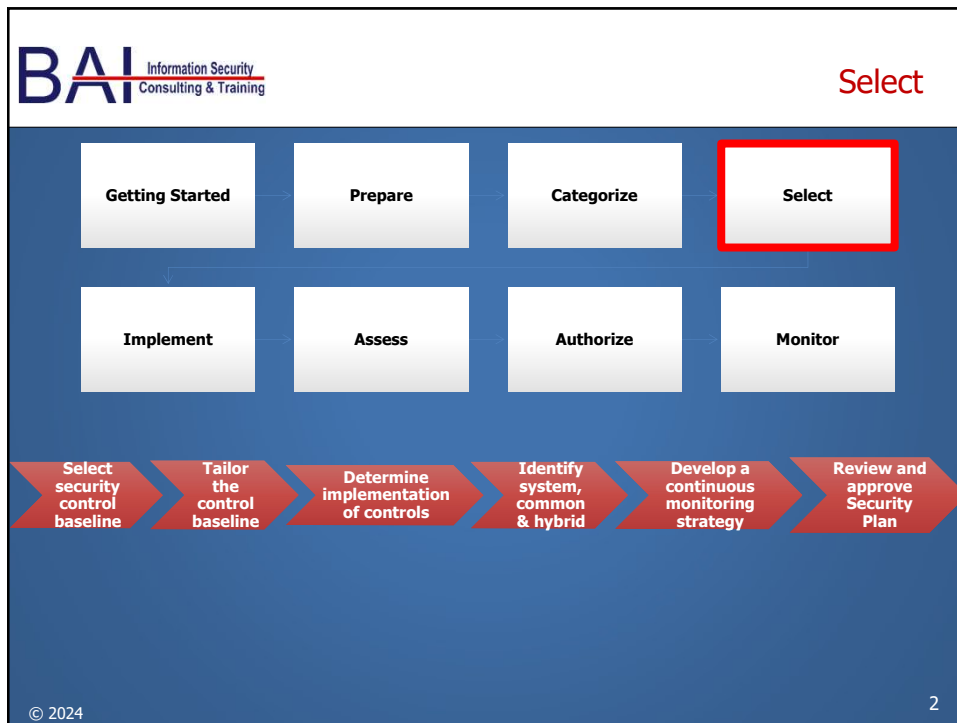


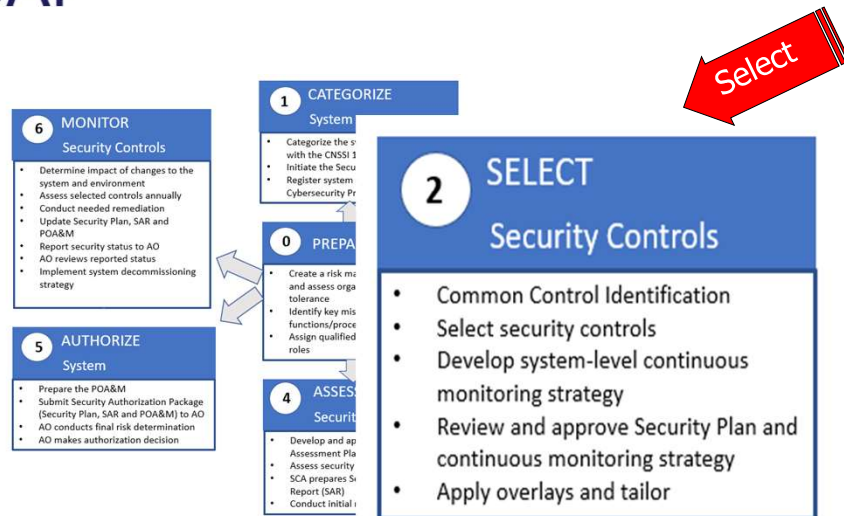


1



2

BAI Where We Are In the RMF for DoD Process



© 2024

Source: DoD Knowledge Service

3

3

BAI Primary Guidance

- RMF Knowledge Service <https://rmfks.osd.mil>
- DoDI 8510.01 RMF for DoD IT
- FIPS Pub 200 Minimum Security Requirements for Federal Information and Information Systems
- CNSSI 1253 Security Categorization and Control Selection for National Security Systems
- NIST SP 800-37 R2, Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy
- NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-53 R5, Security and Privacy Controls for Information Systems and Organizations

© 2024

4

4

BAI NIST SP 800-53 R4 to NIST SP 800-53 R5

Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

Table of Contents

CHAPTER ONE INTRODUCTION 1

1.1 PURPOSE AND APPLICABILITY 2

1.2 TARGET AUDIENCE 3

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS 3

1.4 ORGANIZATIONAL RESPONSIBILITIES 4

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION 6

CHAPTER TWO THE FUNDAMENTALS 7

2.1 MULTITIERED RISK MANAGEMENT 7

2.2 SECURITY CONTROL STRUCTURE 8

2.3 SECURITY CONTROL BASELINES 11

2.4 SECURITY CONTROL DESIGNATIONS 13

2.5 EXTERNAL SERVICE PROVIDERS 14

2.6 ASSURANCE AND TRUSTWORTHINESS 16

2.7 REVISIONS AND EXTENSIONS 26

CHAPTER THREE THE PROCESS 28

3.1 SELECTING SECURITY CONTROL BASELINES 28

3.2 TAILORING BASELINE SECURITY CONTROLS 30

3.3 CREATING OVERLAYS 40

3.4 DOCUMENTING THE CONTROL SELECTION PROCESS 42

3.5 NEW DEVELOPMENT AND LEGACY SYSTEMS 44

APPENDIX A REFERENCES A-1

APPENDIX B GLOSSARY B-1

APPENDIX C ACRONYMS C-1

APPENDIX D SECURITY CONTROL BASELINES – SUMMARY D-1

APPENDIX E ASSURANCE AND TRUSTWORTHINESS E-1

APPENDIX F SECURITY CONTROL CATALOG F-1

APPENDIX G INFORMATION SECURITY PROGRAMS G-1

APPENDIX H INTERNATIONAL INFORMATION SECURITY STANDARDS H-1

APPENDIX I OVERLAY TEMPLATE I-1

APPENDIX J PRIVACY CONTROL CATALOG J-1

BAI NIST SP 800-53 R5

NIST SP 800-53, Rev. 5 SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

Table of Contents

CHAPTER ONE INTRODUCTION 1

1.1 PURPOSE AND APPLICABILITY 2

1.2 TARGET AUDIENCE 3

1.3 ORGANIZATIONAL RESPONSIBILITIES 3

1.4 RELATIONSHIP TO OTHER PUBLICATIONS 5

1.5 REVISIONS AND EXTENSIONS 5

1.6 PUBLICATION ORGANIZATION 5

CHAPTER TWO THE FUNDAMENTALS 7

2.1 REQUIREMENTS AND CONTROLS 7

2.2 CONTROL STRUCTURE AND ORGANIZATION 8

2.3 CONTROL IMPLEMENTATION APPROACHES 11

2.4 SECURITY AND PRIVACY CONTROLS 13

2.5 TRUSTWORTHINESS AND ASSURANCE 14

CHAPTER THREE THE CONTROLS 16

3.1 ACCESS CONTROL 18

3.2 AWARENESS AND TRAINING 59

3.3 AUDIT AND ACCOUNTABILITY 65

3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING 83

3.5 CONFIGURATION MANAGEMENT 96

3.6 CONTINGENCY PLANNING 115

3.7 IDENTIFICATION AND AUTHENTICATION 131

3.8 INCIDENT RESPONSE 149

3.9 MAINTENANCE 162

3.10 MEDIA PROTECTION 171

3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION 179

3.12 PLANNING 194

3.13 PROGRAM MANAGEMENT 203

3.14 PERSONNEL SECURITY 222

3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY 229

3.16 RISK ASSESSMENT 238

3.17 SYSTEM AND SERVICES ACQUISITION 249

3.18 SYSTEM AND COMMUNICATIONS PROTECTION 292

3.19 SYSTEM AND INFORMATION INTEGRITY 332

3.20 SUPPLY CHAIN RISK MANAGEMENT 363

REFERENCES 374

APPENDIX A GLOSSARY 394

APPENDIX B ACRONYMS 424

APPENDIX C CONTROL SUMMARIES 428

© 2024

5

5

BAI New: NIST SP 800-53 R5/SP 800-53B

The future is here!

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

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53r5>

September 2020

NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

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

October 2020

↑ NIST SP 800-53 R5 provides a catalog of security controls

NIST SP 800-53B provides security control baselines for federal civil agencies →

© 2024

6

6

BAI New: NIST SP 800-53 R5

- Content Changes
 - 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
- 20 total families
 - Integrates Privacy within other families (especially PM family) - only one Privacy-pure family
 - Personally Identifiable Information Processing and Transparency (PT)
 - New Supply Chain Risk Management family (SR)

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

© 2024

7

7

BAI NIST SP 800-53 R5 Security Control Families

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

New families:

- ★ Personally Identifiable Information (PII) Processing and Transparency
- ★ Supply Chain Risk Management

© 2024

8

8

BAI Welcome PT Family

Personally Identifiable Information (PII) Processing and Transparency

- **Personally identifiable information** can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- **PII controls implement operations** and evaluate/mitigate operations performed upon PII that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of personally identifiable information.
- **PII processing permissions** are the requirements for how personally identifiable information can be processed or the conditions under which personally identifiable information can be processed.

Note: Many of the previous Privacy controls also integrated into the Program Management (PM) family.

© 2024

9

9

BAI Welcome SR Family

Supply Chain Risk Management

- The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing amount of risk to an organization.
- To address supply chain risks, organizations develop an SCRM policy, which is an important vehicle for directing SCRM activities.
- The policy addresses the goals and objectives in the organization's strategic plan, missions and business functions, and the internal and external customer requirements.
- The SCRM policy defines the SCRM roles and responsibilities within the organization, such as procurement, conducting risk assessments, collecting supply chain threat intelligence, identifying and implementing risk-based mitigations, and performing monitoring functions.

© 2024

10

10

BAI Back to the NIST SP 800-53 R4 to R5

3 Types of DoD Controls

Management: (by Management)

- Of the information system and
- Of risk for a system

Technical: (by Computer system)

- Automated protection (unauthorized access, misuse, help detect security violations)
- Support security requirements for applications and data

Operational: (by People)

- Mechanisms implemented and executed by people
- Often require technical or specialized expertise and rely upon management activities and technical controls

New Management Families
in NIST SP 800-53 R5



© 2024

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

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

11

11

BAI Management Type Control Examples Typically Handled by Management

- CA-5 Plan of Action and Milestones
- CA-7 Continuous Monitoring

- PL-7 Concept of Operations
- PL-8 Security and Privacy Architectures

- RA-2 Security Categorization
- RA-3 Risk Assessment

- SA-16 Developer Provided Training
- SA-21 Developer Screening

- PM-18 Privacy Program Plan
- PM-27 Privacy Reporting
- PT-3 Personally Identifiable Information Processing Purposes
- PT-6 Systems of Records Notice
- SR-2 Supply Chain Risk Management Plan
- SR-7 Supply Chain Operations Security

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



Added In NIST SP 800-53 R5

© 2024

12

12



Technical Type Control Examples Typically Handled by Computer System

- AC-2 Account Management
- AC-5 Separation of Duties
- AC-12 Session Termination
- AC-21 Information Sharing
- AU-3 Content of Audit Records
- AU-8 Time Stamps
- AU-14 Session Audit
- AU-16 Cross-Organizational Audit Logging
- IA-3 Device Identification and Authentication
- IA-5 Authenticator Management
- IA-11 Re-authentication
- SC-2 Separation of System and User Functionality
- SC-5 Denial of Service Protection
- SC-10 Network Disconnect

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

© 2024

13

13



Operational Type Control Examples Typically Handled by People and Rely on Technology

- AT-2 Literacy Training and Awareness
- AT-3 Role-Based Training
- CM-2 Baseline Configuration
- CM-6 Configuration Settings
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- IR-4 Incident Handling
- IR-6 Incident Reporting
- MA-3 Maintenance Tools
- MA-5 Maintenance Personnel
- MP-4 Media Storage
- MP-6 Media Sanitization
- PE-2 Physical Access Authorizations
- PE-8 Visitor Access Records
- PS-3 Personnel Screening
- PS-4 Personnel Termination
- SI-4 System Monitoring
- SI-8 Spam Protection

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

© 2024

14

14

NIST SP 800-53 R4 to R5 – Program Management (PM) – Joins the 20 Families

| CONTROL NUMBER | CONTROL NAME <small>CONTROL ENHANCEMENT NAME</small> |
|----------------|---|
| 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 |
| 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 |

- Deployed organization wide (Tiers 1 & 2)
- Applies to all security control baselines
- Expanded in R5 from PM-16 to PM-32

© 2024

15

15

BAI Privacy Controls

- Based on legislation, policies, guidelines, and best practice
- Independent of categorization
- Select and implement when required for Personally Identifiable Information (PII) or Personal Health Information (PHI)
- Independent of categorization and baseline
- Applies to any system that has privacy information
- Privacy Overlay is the primary means by which controls are added to the baseline
- Reference: NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

© 2024

16

16

BAI 800-53 R4 Appendix J: Privacy Controls

- AP Authority and Purpose
 - AP-1 Authority to Collect
 - AP-2 Purpose Specification
- AR Accountability, Audit, and Risk Management
 - AR-1 Governance and Privacy Program
 - AR-2 Privacy Impact and Risk Assessment
 - AR-3 Privacy Requirements for Contractors and Service Providers
 - AR-4 Privacy Monitoring and Auditing
 - AR-5 Privacy Awareness and Training
 - AR-6 Privacy Reporting
 - AR-7 Privacy-Enhanced System Design and Development
 - AR-8 Accounting of Disclosures
- DM Data Minimization and Retention
 - DM-1 Minimization of Personally Identifiable Information
 - DM-2 Data Retention and Disposal
 - DM-3 Minimization of PII Used in Testing, Training, and Research
- DI Data Quality and Integrity
 - DI-1 Data Quality
 - DI-2 Data Integrity and Data Integrity Board
- IP Individual Participation and Redress
 - IP-1 Consent
 - IP-2 Individual Access
 - IP-3 Redress
 - IP-4 Complaint Management
- SE Security
 - SE-1 Inventory of PII
 - SE-2 Privacy Incident Response
- TR Transparency
 - TR-1 Privacy Notice
 - TR-2 System of Records Notices and Privacy Act Statements
 - TR-3 Dissemination of Privacy Program Information
- UL Use Limitation
 - UL-1 Internal Use
 - UL-2 Information Sharing with Parties

© 2024

17

17

BAI 800-53 R4 Privacy Controls Slide 1 of 2 (Mapping to 800-53 R5)

- **AP Authority and Purpose**
 - **AP-1 Authority to Collect**
 - PT-2 Authority to Process Personally Identifiable Information
 - **AP-2 Purpose Specification**
 - PT-3 Personally Identifiable Information Processing Purposes
- **AR Accountability, Audit, and Risk Management**
 - **AR-1 Governance and Privacy Program**
 - PM-3 Information Security and Privacy Resources
 - PM-18 Privacy Program Plan
 - PM-19 Privacy Program Leadership Role
 - **AR-2 Privacy Impact and Risk Assessment**
 - RA-3 Risk Assessment
 - RA-8 Privacy Impact Assessment
 - **AR-3 Privacy Requirements for Contractors and Service Providers**
 - SA-1 Policies and Procedures
 - SA-4 Acquisition Process
 - SA-9 External System Services
 - **AR-4 Privacy Monitoring and Auditing**
 - CA-2 Control Assessments
 - **AR-5 Privacy Awareness and Training**
 - AT-1 Policies and Procedures
 - AT-2 Literacy Training and Awareness
 - AT-3 Role-Based Training
 - PL-4 Rules of Behavior
 - **AR-6 Privacy Reporting**
 - PM-27 Privacy Reporting
 - **AR-7 Privacy-Enhanced System Design and Development**
 - No specific control mapping but possible discretionary enhancement may pertain, e.g.,
 - PM-20(1) Privacy Policies on Websites, Applications and Digital Services
 - **AR-8 Accounting of Disclosures**
 - PM-21 Accounting of Disclosures
- **DI Data Quality and Integrity**
 - **DI-1 Data Quality**
 - PM-22 Personally Identifiable Information Quality Management
 - SI-18 Personally Identifiable Information Quality Operations
 - **DI-2 Data Integrity and Data Integrity Board**
 - PM-24 Data Integrity Board
 - SI-1 Policies and Procedures
- **DM Data Minimization and Retention**
 - **DM-1 Minimization of Personally Identifiable Information**
 - PM-5(1) System Inventory/Inventory of Personally Identifiable Information
 - SA-8 (33) Security and Privacy Engineering Principles/Minimization
 - SI-12(1) Information Management & Retention/Limit Personally Identifiable Information Elements
 - **DM-2 Data Retention and Disposal**
 - MP-6 Media Sanitization
 - SI-12 Information Management & Retention
 - SI-12(3) Information Disposal

© 2024

18

18

BAI 800-53 R4 Privacy Controls Slide 2 of 2 (Mapping to 800-53 R5)

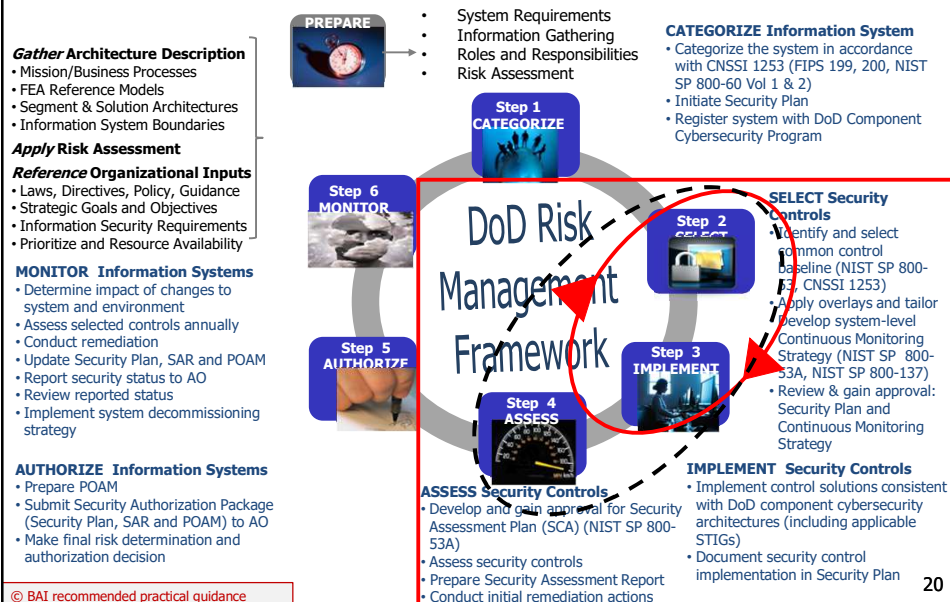
- **DM-3 Minimization of PII Used in Testing, Training, and Research**
 - PM-25 Minimization of Personally Identifiable Information in Testing, Training and Research
 - SI-12(2) Information Management & Retention/Minimize Personally Identifiable Information in Testing, Training and Research
- **IP Individual Participation and Redress**
 - **IP-1 Consent**
 - PT-4 Consent
 - **IP-2 Individual Access**
 - AC-1 Policies and Procedures
 - AC-3(14) Access Enforcement/Individual Access
 - PM-20 Dissemination of Privacy Program Information
 - PT-5 Privacy Notice
 - PT-6 System of Records Notice
 - **IP-3 Redress**
 - PM-22 Personally Identification Information Quality Management
 - SI-18 Personally Identifiable Information Quality Operations
 - SI-18(4) Individual Requests
 - SI-18(5) Notice of Correction or Deletion
 - **IP-4 Complaint Management**
 - PM-26 Complaint Management
- **SE Security**
 - **SE-1 Inventory of PII**
 - PM-5(1) System Inventory/Inventory of Personally Identifiable Information
 - **SE-2 Privacy Incident Response**
 - IR-8 Incident Response Plan
 - IR-8(1) Breaches
- **TR Transparency**
 - **TR-1 Privacy Notice**
 - PT-5 Privacy Notice
 - PT-5(1) Just-in-time Notice
 - **TR-2 System of Records Notices and Privacy Act Statements**
 - PT-5(2) Privacy Notice/Privacy Act Statements
 - PT-6 System of Records Notice
 - **TR-3 Dissemination of Privacy Program Information**
 - PM-20 Dissemination of Privacy Program Information
- **UL Use Limitation**
 - **UL-1 Internal Use**
 - PT-3 Personally Identifiable Information Processing Purposes
 - **UL-2 Information Sharing with Parties**
 - AC-21 Information Sharing
 - AT-3(5) Role-Based Training/Processing Personally Identifiable Information
 - AU-2 Event Logging
 - PT-2 Authority to Process Personally Identifiable Information
 - PT-3 Personally Identifiable Information Processing Purposes

© 2024

19

19


BAI BAI Practical Guidance - Plan to Tightly Couple Select, Implement and Assess



20

20

Next...
Analysis of Individual Security Controls



21

21

BAI

Security Control Structure Example: AU-5 Response to Audit Logging Process Failures

| | |
|---------------------------------|---|
| Control ID and name | AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES |
| Control Description | Control: a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time-period] in the event of an audit logging process failure; and |
| Organization Defined Parameters | b. Take the following additional actions: [Assignment: organization-defined additional actions]. |
| Discussion | Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel. Related Controls: AU-2 , AU-4 , AU-7 , AU-9 , AU-11 , AU-12 , AU-14 , SI-4 , SI-12 . |
| References | References: None |

© 2024

Source: NIST SP 800-53 R5

22

22

BAI

Security Control Structure Example: AU-5 Response to Audit Logging Process Failures (Control Enhancements)

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Control Enhancements:

(1) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | STORAGE CAPACITY WARNING
Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.

(2) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | REAL-TIME ALERTS
Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].

(3) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS
Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.

(4) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | SHUTDOWN ON FAILURE
Invoke a [Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available] in the event of [Assignment: organization-defined audit logging failures], unless an alternate audit logging capability exists.

(5) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | ALTERNATE AUDIT LOGGING CAPABILITY
Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [Assignment: organization-defined alternate audit logging functionality].

© 2024

Source: NIST SP 800-53 RS

BAI

Additional Control Information

CP-6 ALTERNATE STORAGE SITE

Control:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Discussion: Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls:

- CP-2 Contingency Plan
- CP-9 System Backup
- MP-4 Media Storage

References:

- E.g., NIST SP 800-34 Contingency Planning Guide





Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

References: [SP 800-34].

© 2024

Source: NIST SP 800-53 RS

BAI Identifying Control Requirements

- NIST SP 800-53 R4/R5
 - What does the control statement mean? 
 - To what part(s) does it apply? 
 - How is the control implemented? 
- NIST SP 800-53A R4/R5
 - How are the control requirements assessed? 

© 2024

25

25

BAI CCI's and Requirements (for DoD systems)

- Control Correlation Identifier (CCI)
 - NIST SP 800-53A controls and enhancements are subdivided into individual statements.
 - Statements labeled with Control Correlation Identifier (CCI) number in eMASS, Knowledge Service, automated tools.
- Example CCI: CCI-000110
 - Control Number AT-3 Role-Based Training
 - CCI Definition: The organization provides refresher role-based security training to personnel with assigned security roles and responsibilities in accordance with organization-defined frequency.
 - Implementation Guidance: Privileged user type security-related education/training available through DISA or other professional resources meets the provision of this control.
 - Assessment: The organization conducting the inspection/assessment obtains and examines documented records of their privileged users training.

© 2024

26

26

BAI What does the control mean? Where does the control apply?

Meaning and Intent

- What is the control seeking to protect?
 - Confidentiality
 - Integrity
 - Availability
- How they support operations
- How they can be tailored

Applies to Which Part(s)?

- Across the whole organization, e.g., policy
- Component by component, e.g., access control, number of failed logons
- Personnel
- Facility (physical)
- Hardware
 - Servers
 - Workstations
 - Network (firewall, router)
- Software
 - Operating System
 - Database
 - Web Server
 - Applications

© 2024

27

27

BAI How to Implement and Assess the Control

How to implement?



- Technical
 - Apply security guidelines
 - Update system software
 - Re-engineer systems
- Documentation/Artifacts
 - Policies and Procedures
 - Local Security Plans (e.g., Contingency, Incident)
 - Logs
 - Document compliance
- Inherit from provider
- Compensating controls

How to assess?



- Examine - Review, inspect, observe, study (e.g., policies, procedures, system backups, authenticating)
- Interview - To understand, clarify, or obtain evidence (e.g., privileged account protection, system failures)
- Test - Under specified conditions to compare actual with expected behavior (e.g., show procedure for unlocking an account)

Next... An example Operational Control: CM-3 Configuration Change Control

© 2024

28

28

BAI CM-3 Operational Control Example

CM-3 CONFIGURATION CHANGE CONTROL

a. Determine and document the types of changes to the system that are configuration-controlled;

- Means-identify what types of changes are configuration controlled for system components
 - Normal change
 - Standard change
 - Emergency change
 - Other Agency-defined changes (e.g., No-impact changes, Urgent changes, etc.)

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

- Means:
 - System modifications are reviewed against policies and standards
 - Impact to system risk determines whether changes are approved.

c. Document configuration change decisions associated with the system;

- Means:
 - Changes to the system are documented in change control logs
 - The system has an established configuration management and change management program
 - Configuration Control Board decisions are properly documented

d. Implement approved configuration-controlled changes to the system;

- Means:
 - Approved changes are implemented

© 2024

Source: NIST SP 800-53 R5

29

29

BAI CM-3 Operational Control Example

e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];

- Means:
 - Documentation of system modifications are retained throughout the system lifecycle
 - Configuration documentation is reviewed for accuracy
 - Records of system reviews are retained

f. Monitor and review activities associated with configuration-controlled changes to the system;

- Means:
 - Personnel are assigned to periodically review and audit system change records on a regular basis
 - Results of audit and reviews are recorded
 - System documentation is updated as required

g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].

- Means:
 - Establish a configuration management oversight structure [organization-defined (e.g., committee; board, etc.)]
 - Board meets on an established basis [organization-defined (e.g., weekly, etc.)]
 - Board meets based on [organization-defined] criteria [organization-defined conditions (e.g., emergency changes needed; system compromised, etc.)]

© 2024

30

30

BAI To Which Part(s) Does CM-3 APPLY?

Operational Control Example

- CM-3 Configuration Change Control applies to all components within the system boundary
 - Hardware
 - Servers
 - Workstations
 - Network
 - System Software
 - Operating Systems
 - Database
 - Web Servers
 - Applications
 - Documentation





© 2024

31

31

BAI How to Implement and Assess CM-3

Operational Control Example

| How to implement | How to assess |
|---|--|
| <ul style="list-style-type: none"> • Develop Configuration Management (CM) plan • Establish Configuration Control Board (CCB) • Formally track and document changes • Train administrators to comply with CM Plan  | <p>Examine:</p> <ul style="list-style-type: none"> • Examine documentation for standard methods for CM • Verify change control logs are maintained • Review CCB records <p>Interview</p> <ul style="list-style-type: none"> • Security Officer to determine knowledge and understanding of CM process • System Administrators (Network, Database, Web) to verify proper implementation of CM process <p>Test</p> <ul style="list-style-type: none"> • Using automated tools, verify consistent system configuration management  |

© 2024

Artifacts: Configuration Management Plan; CCB Charter; CCB Meeting Minutes; System Change Requests; CCB decisions tracked in automated tool

32

32

BAI What does CA-5 Plan of Action and Milestones MEAN?

CA-5 PLAN OF ACTION AND MILESTONES

Management Control Example

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system;

Means:

- Develop POAM
- Track weaknesses
- Assign responsibilities
- Determine resources required to mitigate weaknesses
- Establish milestones reduce or eliminate weaknesses

b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Means:

- Review and update the POAM based on pre-determined timeframe
- Establish procedures to ensure POAM review is incorporated during continuous monitoring System Development Life Cycle

© 2024

Source: NIST SP 800-53 R5

33

33

BAI CA-5 Plan of Action and Milestones

Management Control Example

IMPLEMENT CA-5

- Develop POAM in accordance with OMB 03-19 or local policy
- Establish processes to ensure risk remediation is properly documented
- Assign responsibility for managing and tracking risk
- Conduct consistent periodic POAM reviews



ASSESS CA-5

Examine:

- Verify POAM exists
- Review POAM for accuracy
- Local policy and procedures for tracking risk

Interview:

- System Owner to verify understanding of risk management
- Security Officer to determine consistent method for documenting risk



Artifacts: Document that further explains POA&M process and POA&M development.

© 2024

34

34

BAI AU-5 Technical Control Example

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Technical Control Example

a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure.

Means:

- Processes and procedures are in place to alert personnel in response to audit processing alerts

b. Take the following additional actions: [Assignment: organization-defined additional actions].

Means:

- Shutdown system
- Overwrite oldest audit records
- Stop generating records

© 2024

Source: NIST SP 800-53 R5

35

35

BAI AU-5 APPLIES to What Part(s)?

Technical Control Example

- AU-5 Response to Auditing Process Failures applies to:
- All IT components within the system boundary
 - Windows/Linux/Solaris Servers
 - Workstations
 - Routers/Firewalls/Switches
 - Database Servers
 - Web Servers
 - Applications
- May apply to other components
 - Building access systems
 - HVAC

© 2024

36

36

BAI AU-5 Control Enhancements

(1) Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.

Technical Control Example

(2) Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].

Implement

- Ensure systems are configured to collect and retain audit information
- Establish alert processes and procedures
- Develop policies and procedures to respond to audit alerts



Assess

- Examine
 - Audit records to verify proper content
 - Audit response policies and procedures
 - Verify all components are included in the reporting plan
- Interview
 - System Administrators and personnel responsible for monitoring audit records to verify understanding of reporting procedures



© 2024

37

37

BAI Course Activity

- Refer to Course Guide "Identify PCOMS Security Control Requirements"



© 2024

38

38

BAI REVIEW

- What are some examples of control families in the NSS and NIST control baselines?
- What drives the flexibility of the RMF controls?
- What are some examples of organization defined parameters?
- What are the four elements of dissecting a security control? You need to think about what?
- What are the three primary ways you can assess a control?



© 2024

Next... The Select Process

39

39

BAI Select the Baseline



© 2024

40

40



DoD or NSS Control Baseline - CNSSI 1253, Appendix D

CNSSI Appendix D aligns security control by CIA

Key:

- "X" is NIST Non NSS baseline
- "+" for NSS supplements NIST
- "X" and "+" create NSS Baseline

| ID | Title | Privacy Control Baseline | Privacy Implementation Considerations | Security Control Baselines | | | | | | | | |
|----------|--|--------------------------|---------------------------------------|----------------------------|---|---|---|---|---|---|---|---|
| | | | | C | | | I | | | A | | |
| | | | | L | M | H | L | M | H | L | M | H |
| AC-1 | Policy and Procedures | X | | X | X | X | X | X | X | X | X | X |
| AC-2 | Account Management | | | X | X | X | X | X | X | | | |
| AC-2(1) | Automated System Account Management | | | X | X | | X | X | | | | |
| AC-2(2) | Automated Temporary and Emergency Account Management | | | X | X | | X | X | | | | |
| AC-2(3) | Disable Accounts | | | X | X | | X | X | | | | |
| AC-2(4) | Automated Audit Actions | | | + | X | X | + | X | X | | | |
| AC-2(5) | Inactivity Logout | | | + | X | X | + | X | X | + | X | X |
| AC-2(6) | Dynamic Privilege Management | | | | | | | | | | | |
| AC-2(7) | Privileged User Accounts | | | + | + | + | + | + | + | | | |
| AC-2(8) | Dynamic Account Management | | | | | | | | | | | |
| AC-2(9) | Restrictions on Use of Shared and Group Accounts | | | + | + | + | + | + | + | | | |
| AC-2(11) | Usage Conditions | | | | | X | | | X | | | X |
| AC-2(12) | Account Monitoring for Atypical Usage | | √ | + | + | X | + | + | X | | | |
| AC-2(13) | Disable Accounts for High-Risk Individuals | | | + | X | X | + | X | X | | | |

© 2024 Source: CNSSI 1253, July 2022

41

41



Select the NSS/DoD Control Baseline – Additional Controls

- Available extra controls
- Added protection
- Support special requirements

| ID | Title | Privacy Control Baseline | Privacy Implementation Considerations | Security Control Baselines | | | | | | | | |
|----------|--|--------------------------|---------------------------------------|----------------------------|---|---|---|---|---|---|---|---|
| | | | | C | | | I | | | A | | |
| | | | | L | M | H | L | M | H | L | M | H |
| SC-30(5) | Concealment of System Components | | | | | | | | | | | |
| SC-31 | Covert Channel Analysis | | | | | | | | | | | |
| SC-31(1) | Test Covert Channels for Exploitability | | | | | | | | | | | |
| SC-31(2) | Maximum Bandwidth | | | | | | | | | | | |
| SC-31(3) | Measure Bandwidth in Operational Environments | | | | | | | | | | | |
| SC-32 | System Partitioning | | | | | | | | | | | |
| SC-32(1) | Separate Physical Domains for Privileged Functions | | | | | | | | | | | |

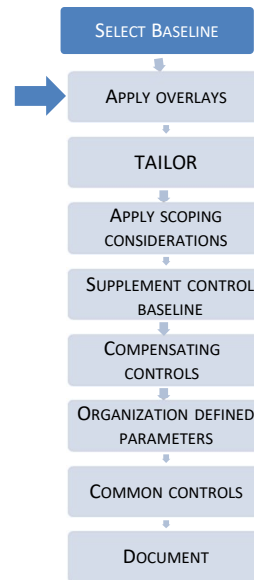
© 2024

42

42

BAI Select – Apply Overlays

- Define baseline independent specifications of controls and supporting guidance to:
 - Complement baselines
 - Address additional factors
- Use overlays to:
 - Provide consistency among similar systems
 - Promote reciprocity



© 2024

43

43

BAI Apply or Create Overlay

- CNSSI 1253 Appendix F lists Federal Overlays on the www.cnss.gov website.
- Current Approved List:
 - Security Overlay template (12/12/2022)
 - Space Platform Overlay (02/23/2018)
 - Cross Domain Solution Overlay (02/08/2023) (Document is U/FOUO)
 - Intelligence Overlay (04/19/2016) (Document is U/FOUO)
 - Classified Information Overlay (09/30/2022)
 - Privacy Overlay (04/23/2015) (new update pending)
- Examples of other organizational available overlays:
 - DoD Financial Management (FM) Overlay (on the DoD Knowledge Service)
 - Guide to Operational Technology (OT) Security (included in NIST SP 800-82, Sep 2023)

© 2024

44

44

BAI Useful Categories to Create Overlays

- Communities of interest:
 - Industry sectors, or coalitions/ partnerships
 - Healthcare, law enforcement, financial, transportation, energy, allied collaboration/sharing)
- Information technologies/ computing paradigms
 - Cloud/mobile, PKI, Smart Grid
- Environments of operation
 - Tactical
- Types of information systems and operating modes
 - Weapons systems, single-user systems, standalone systems
- Types of missions/operations
 - Counterterrorism, first responders, research, development, test, and evaluation
- Statutory/regulatory
 - Foreign Intelligence Surveillance Act, Health Insurance Portability and Accountability Act

© 2024

45

45

BAI Overlay Example: Privacy

- CNSSI No.1253F, Attachment six
- Privacy Overlay - Consists of four Privacy Overlays:
 - Protected Health Information (PHI)
 - Personally Identifiable Information (PII) Low
 - Personally Identifiable Information (PII) Moderate
 - Personally Identifiable Information (PII) High

Table 3: Privacy Overlays Security and Privacy Controls

| CONTROL | PRIVACY OVERLAYS | | | |
|----------|----------------------------------|----------|-------|------|
| | PII Confidentiality Impact Level | | | PHI |
| | LOW | MODERATE | HIGH | |
| AC-1 | +GR | +GR | +GR | +ER |
| AC-2 | +EGVR | +EGVR | +EGVR | +EGR |
| AC-2(8) | | --R | --R | |
| AC-2(9) | GVR | GVR | GVR | R |
| AC-2(13) | +R | +R | +R | +R |
| AC-3 | +EGR | +EGR | +EGR | +GR |
| AC-3(9) | | +EVR | +EVR | +R |
| AC-3(10) | GVR | GVR | GVR | |
| AC-4 | | +GR | +GR | +R |

| | |
|----|---|
| + | Select this control (Required) |
| -- | Do NOT select this control (Required) |
| E | There is a control extension |
| G | Supplemental guidance, including specific tailoring guidance if applicable, for the control. |
| V | Defines a value for an organizational-defined parameter for the control. |
| R | One (or more) regulatory/ statutory reference(s) require the control, the control helps meet regulatory/statutory requirements. |

© 2024 Control is only required when "+" or a "--" is indicated.

46

46

BAI DoD Financial Management (FM) Overlay



KNOWLEDGE
SERVICE

RMF Implementation

RMF for DoD Technology

Controls and Authorization

RMF Policy and Governance

Collaboration

RMF KS > Controls and Authorization > DoD FM Overlay > FM Overlay Summary

FM Overlay Summary

FM Overlay Summary Table

The **FM Overlay Summary Table** identifies the baseline and optional NIST controls that are in the FM Overlay. It leverages FISCAM Appendix IV, Mapping FISCAM to NIST SP 800-53 and other related NIST Publications. In some cases, the application of the FM Overlay will force the inclusion of RMF controls that would not otherwise have been selected based on the results of system categorization.

- A plus sign (+) indicates the RMF security control is designated a baseline control. Baseline controls are shown in **bold font**.
- A minus sign (-) indicates that the RMF security control is designated as optional. Optional controls are shown in normal (unbolded) font.
- Two dashes (--) indicate that the RMF security control is neither required nor optional for the FM Overlay.

In addition, each control in the FM Overlay Summary Table is encoded to assist FM Overlay users in identifying controls for which the FM Overlay provides additional guidance, specific parameters, or regulatory requirements:

- The letter E indicates there is a control extension.
- The letter G indicates there is supplemental guidance, including specific tailoring guidance, if applicable, for the control.
- The letter V indicates this Supplemental Guidance defines a value for an organizationally defined parameter for the control.
- The letter R indicates there is at least one regulatory or statutory reference that requires or prohibits the control selection or that the control helps to meet the regulatory or statutory requirements.

| Row | Control | FM Overlay | Control | FM Overlay | Control | FM Overlay |
|-----|-----------|------------|-----------|------------|-----------|------------|
| 1 | AC-1 | +EG | AC-2 | +EG | AC-2 (1) | +EG |
| 2 | AC-2 (2) | +EG | AC-2 (3) | +EG | AC-2 (4) | +EG |
| 3 | AC-2 (5) | +EG | AC-2 (6) | +EG | AC-2 (7) | +EG |
| 4 | AC-2 (8) | +EG | AC-2 (9) | +EG | AC-2 (10) | +EG |
| 5 | AC-2 (11) | +EG | AC-2 (12) | +EG | AC-2 (13) | +EG |
| 6 | AC-3 | +EG | AC-3 (2) | +EG | AC-3 (3) | +EG |
| 7 | AC-3 (4) | +EG | AC-3 (5) | +EG | AC-3 (7) | +EG |

© 2024

47

47

BAI Operational Technology (OT) Manual Overlay example

NIST Special Publication
NIST SP 800-82r3

Guide to Operational Technology (OT) Security

| CNTL NO. | CONTROL NAME | INITIAL CONTROL BASELINES | | |
|----------|--|---------------------------|-----------------------|----------------------------|
| | | LOW | MOD | HIGH |
| CM-10 | Software Usage Restrictions | CM-10 | CM-10 | CM-10 |
| CM-11 | User-Installed Software | CM-11 | CM-11 | CM-11 |
| CM-12 | Information Location | | CM-12 (1) | CM-12 (1) |
| CP-1 | Policy and Procedures | CP-1 | CP-1 | CP-1 |
| CP-2 | Contingency Plan | CP-2 | CP-2 (1) (3) (8) | CP-2 (1) (2) (3) (5) (8) |
| CP-3 | Contingency Training | CP-3 | CP-3 | CP-3 (1) |
| CP-4 | Contingency Plan Testing | CP-4 | CP-4 (1) | CP-4 (1) (2) |
| CP-6 | Alternate Storage Site | | CP-6 (1) (3) | CP-6 (1) (2) (3) |
| CP-7 | Alternate Processing Site | | CP-7 (1) (2) (3) | CP-7 (1) (2) (3) (4) |
| CP-8 | Telecommunications Services | | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) |
| CP-9 | System Backup | CP-9 | CP-9 (1) (3) | CP-9 (1) (2) (3) (5) (8) |
| CP-10 | System Recovery and Reconstruction | CP-10 | CP-10 (2) (4) | CP-10 (2) (4) (8) |
| CP-12 | Safe Mode | CP-12 | CP-12 | CP-12 |
| IA-1 | Policy and Procedures | IA-1 | IA-1 | IA-1 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (1) (2) (8) (12) | IA-2 (1) (2) (8) (12) | IA-2 (1) (2) (8) (12) (12) |
| IA-3 | Device Identification and Authentication | IA-3 | IA-3 | IA-3 |

Appendix F – OT Overlay

Underlines indicate added controls

CP-12 SAFE MODE

| CNTL NO. | CONTROL NAME Control Enhancement Name | SUPPLEMENTED CONTROL BASELINES | | |
|----------|--|--------------------------------|-------|-------|
| | | LOW | MOD | HIGH |
| CP-12 | Safe Mode | Added | Added | Added |

ICS Supplemental Guidance: The organization-defined conditions and corresponding restrictions of safe mode of operation may vary among baselines. The same condition(s) may trigger different response depending on the impact level. The conditions may be external to the ICS (e.g., electricity supply brown-out). Related controls: SI-17.

Rationale for adding CP-12 to all baselines: This control provides a framework for the organization to plan their policy and procedures for dealing with conditions beyond their control in the environment of operations. Creating a written record of the decision process for selecting incidents and appropriate response is part of risk management in light of changing environment of operations.

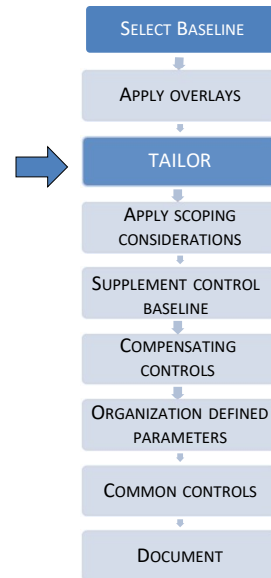
© 2024

48

48

BAI Select - Tailoring Process

- Gives organizations flexibility to adapt to:
 - Missions/business functions
 - Information systems
 - Environments of operation
- Identify added assurance—related controls to increase the level of trustworthiness



© 2024

49

49

BAI RMF Tailoring Process – Apply Scoping Considerations

- AO's must approve before controls are implemented
- Be sure to document and provide rationale for affected security controls
- When applied with risk management, scoping helps:
 - Eliminate unnecessary security controls
 - Ensure organizations include only those controls needed
 - Example: Applications or unique PIT systems may not require:
 - AC-18 Wireless Access
- Technology: Apply controls only if relevant, e.g., wireless, VOIP
- Mission Requirements, E.g., uninterrupted display required (such as air traffic control) may exclude:
 - AC-11 Device Lock
 - SC-10 Network Disconnect

© 2024

50

50

BAI Scoping Considerations Operational/Environmental

- Data Connectivity and Bandwidth, e.g., air gapped (not networked) may exclude:
 - AC-17 Remote Access
 - SC-8 Transmission Confidentiality and Integrity
 - SC-7 Boundary Protection
- Operational/Environmental
 - Public Access might exclude these controls:
 - AC-7 Unsuccessful Logon Attempts
 - AC-17 Remote Access
 - IA-2 Identification and Authentication
 - IA-4 Identifier Management
 - IA-5 Authenticator Management
- Non-persistence* (Information and/or Information System), e.g., tactical systems, industrial control systems might exclude:
 - CP-6 Alternate Storage Site
 - CP-7 Alternate Processing Site
 - CP-9 System Backup
 - MP-6 Media Sanitization
 - SC-28 Protection of Information at Rest

*Versus persistent data that has a relatively long duration (days, weeks.)

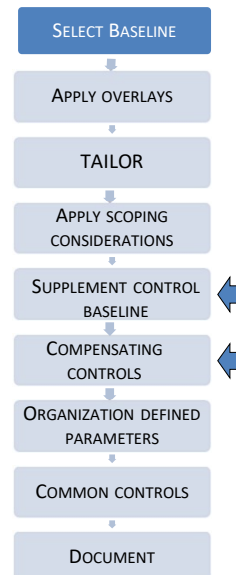
© 2024

51

51

BAI Select Compensating Controls and Supplement the Baseline

- Supplement Control Baseline
 - Depends on organization's assessment of risk
 - Mitigate baseline with supplemented (additional) controls
 - Reference the Discussion "Related Controls" for guidance on which controls can be used to supplement
- Compensating controls:
 - Alternative controls that can provide equivalent or comparable protection
 - AC-5 Separation of Duties may be compensated with strengthening audit, accountability and personnel controls
 - Document rationale and how risk has been assessed and accepted



© 2024

52

52



Define Requirements and Analyze Gaps When Supplementing with Added Controls

Define Requirements

- Identify threats
 - Is it credible?
 - Is information specific?
 - Are assumptions needed?
 - Then establish requirements

Analyze Gaps

- Do an organizational assessment of current defensive capability or cyber preparedness
- Determine gaps to determine risk

© 2024

53

53



Situations that Require Supplementing Examples

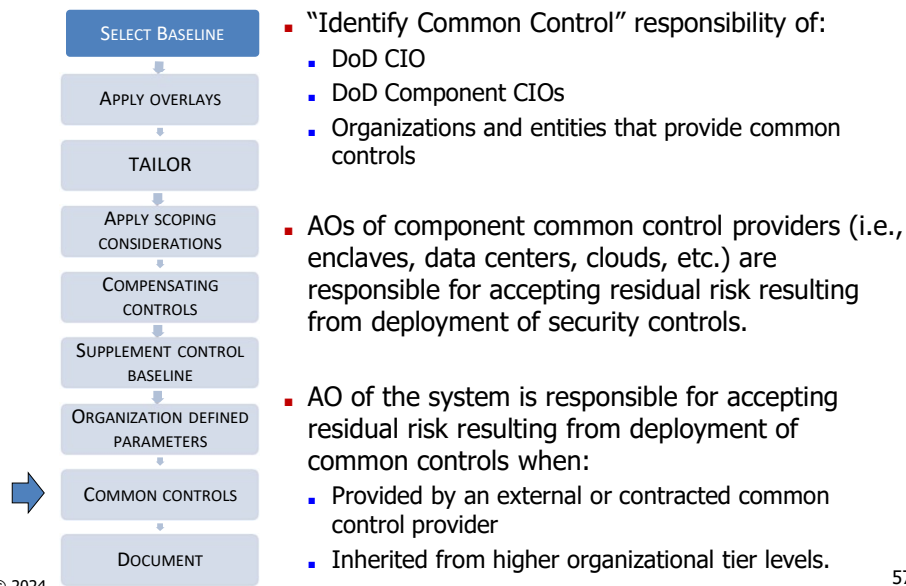
- Situation: Advanced persistent threat (APT) – adversaries have a foothold. Consider:
 - CM-5(4) Access Restrictions for Change – Dual Authorizations
 - SC-7(13) Boundary Protection | Isolation of security tools/Mechanisms/Support Components (Segmentation)
- Situation: Mobility/Mobile Devices. Consider:
 - AC-7(2) Unsuccessful Logon Attempts | Purge or Wipe Mobile Device
 - MP-6(8) Media Sanitization | Remote Purging or Wiping of Information
- Situation: Classified or Sensitive information - users do not all have authorization. Consider:
 - AC-3(3) Access Enforcement | Mandatory Access Control
 - MA-5(4) Maintenance Personnel | Foreign Nationals

© 2024

54

54

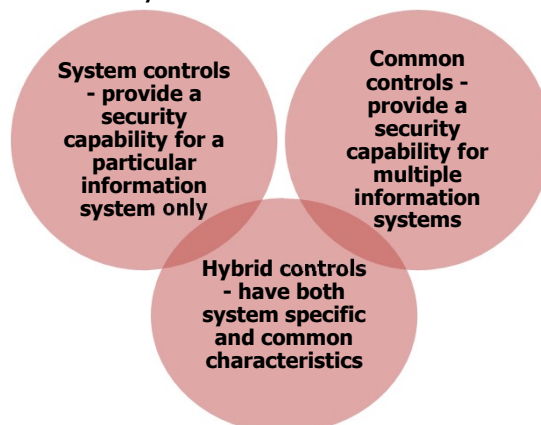
BAI Identify Common Controls



57

BAI Common vs. Hybrid Controls

- Common: inherited by one or more information systems
- Organization determines which to implement
- Implementation may reduce costs



© 2024

Source: NIST SP 800-53 R5, Section 2.3

58

58

BAI Common Controls Requirements -> Analysis -> Control

Determine Requirement: Facility that houses system must have fire alarms



Do Analysis: System is located in government data center



Select Common Controls:
System inherits control status from data center system owner

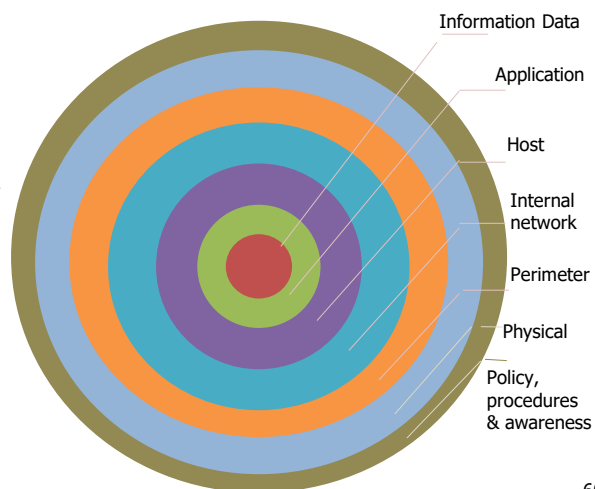
© 2024

59

59

BAI Example Common Controls and Defense in Depth – Layers of Protection

- Common controls:
 - Heating, Ventilation, and Cooling (HVAC)
 - Personnel Security (Clearances, Badges)
 - Physical Security (Gates, Guards)
 - Agency/Department wide security policies
 - Perimeter—network boundary defenses
- System defined in SSP
 - System Owner and Security Officer review the controls
 - System Owner and Security Officer identify “Common Controls” that can be applied to the system



© 2024

60

60

BAI Who Has Responsibility?

Resident Controls

- Controls that reside in an Information System (IS)
 - Hardware and Operating System for a hosted system
 - Vulnerability Scanning
 - Telecommunications
- Providers may also be the information system owners

Non-Resident controls

- External to the IS
 - Physical and environmental protection controls
 - Personnel security controls
- Organization selects senior organizational official(s) or executive(s) as authorizing officials for those controls



Ensure common control providers have capability to broadcast control status changes quickly

© 2024

61

61

BAI

- SITUATION: The Common Control Provider is not fully implementing one or more common controls.
- What recourse does a system owner have?



© 2024

62

62

BAI Select Process Course Activity

- Refer to Course Guide "Allocate Security Controls"



© 2024

63

63

BAI Example Justification Statement

- Justification is required whenever tailoring the baseline
- Example Justification Statement
- Source: Privacy Overlay

AC-2, ACCOUNT MANAGEMENT

Control Enhancement: 13

Justification to Select: Disabling accounts for high-risk individuals is a minimum requirement for the organization's rules of behavior because of abusing access privileges to access PII, including information protected under the Privacy Act of 1974.

© 2024

64

64

BAI Example Justification Statement

- Example Justification Statement
- Source: Classified Information

AC-3, ACCESS ENFORCEMENT

Control Enhancement: 2

Justification to Select: White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, requires the implementation of two-stage controls (review and concurrence of a second person) for all transfers of data from a classified computer network to removable media, if the transfer is not part of an approved internal use process such as encrypted back-ups.

© 2024

65

65

BAI Continuous Monitoring Plan



- Must be done in response to FISMA requirements
 - Annual updated results at a minimum
 - Security control assessments
 - Continuous monitoring activities
 - Software Development Life Cycle (SDLC) or audit testing and evaluation
- Goal is to manage risk
 - Officials need to make informed risk management decisions
 - Risk (categorization/impact) determines rigor and frequency
 - Subsets of all controls must be assessed annually

© 2024

66

66

BAI Continuous Monitoring Plan

- Continuous monitoring system-level strategy
 - Monitors effectiveness of security controls
 - Leverages automated data feeds
 - Quantifies security metrics
 - Enables prioritization for mitigation/remediation
 - Identifies deviations from expected results
 - Monitors actual or proposed changes and operational environments including inherited controls
 - Included as an artifact to the Security Plan

© 2024

67

67

BAI Considerations

- Identify specific security controls monitoring frequency
 - Assess volatile or critical controls more often
 - Review risk assessment for high-level concerns tied to controls
 - Prioritize controls for monitoring based on risk
 - Factor in trustworthiness of common control provider when reviewing frequency of common controls assessment
 - Use metrics and review trends
- Identify when to change frequency
 - New regulatory requirements
 - A security incident
 - Changes in the IT environment
 - Review of trends identifies potential problem

© 2024

68

68

BAI Plan Must Align to Information System Continuous Monitoring (ISCM) Strategy

- Critical management function—not just IT
- RMF requires organization and system level strategy
- System level role and strategy:
 - Conform to Tier 1 requirements
 - Relies on manual and automated assessment
- AO reviews/approves


See also: NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

© 2024 69


69

BAI Use RMF Assessment Techniques


- Consider Assessment techniques for the ISCM plan
- Helps ensure more efficient control implementation



EXAMINE Review, observe, analyze assessment objects (i.e., specifications, mechanisms, or activities) to facilitate assessor understanding, clarification, or obtain evidence.



INTERVIEW Conduct discussions with individuals or groups to facilitate understanding, clarification, or obtain evidence.



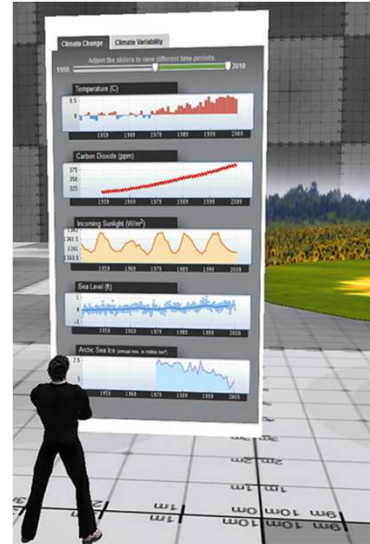
TEST Run assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior. Examples: automated test tools output, system configuration screen shots.

© 2024 70

70

BAI Planning System Level Metrics

- Automation is encouraged
- Not feasible for most controls
- Information on control assessments must be actionable
- Standard set of data elements for an Incident Response tracking system*
 - When incident is reported: reporter's name, phone number, and location
 - Incident handler: Name – Role – Organizational unit (e.g., agency, department, division, team) and affiliation
 - Incident details: Status change date/timestamps, physical location



© 2024 *Source: NIST SP 800-61 Computer Security Incident Handling Guide

71

71

BAI Meaningful Metrics: IR-6

Incident Reporting (IR) IR-6

- a. Require personnel to report suspected incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*];
- b. Report incident information to [*Assignment: organization-defined authorities*].

- Examples of actionable data (time):
 - How long it took the IR team to respond to the initial incident report
 - How long to report to management (and as appropriate, others)
- Objective assessment:
 - Determine adherence to established IR policies and procedures
 - Did damage occur
- Report on the attack itself:
 - Whether it is a recurrence of a previous incident
 - Calculating the estimated monetary damage from the incident
- Identifying any measures that might have prevented the incident

© 2024

72

72

BAI Metrics that Matter

- Characteristics of helpful metrics
 - Automated assessments typically more cost effective, efficient and consistent
 - Manual assessments must be consistent, repeatable and verifiable
 - Sustainable? Can it be repeated regularly?
 - Provide trend analysis. Absolute values not as helpful as those that indicate a trend

© 2024

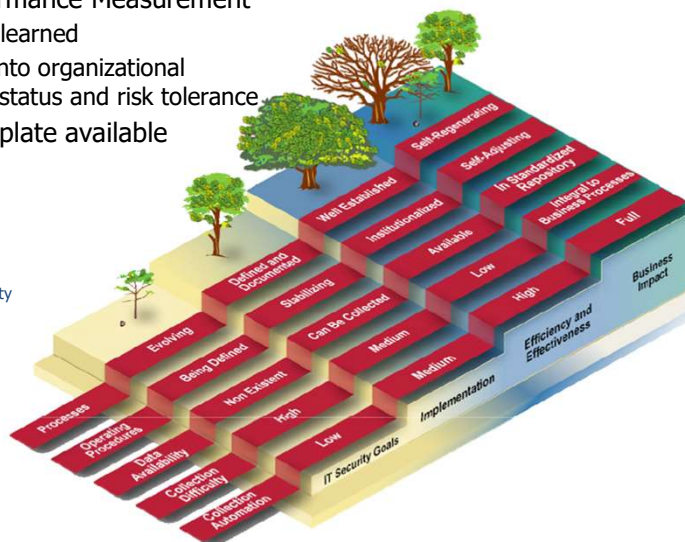
73

73

BAI Measuring Program Effectiveness

- NIST Performance Measurement
 - Lessons learned
 - Insight into organizational security status and risk tolerance
- Metrics template available

Ref: NIST SP 800-55
Performance Measurement
Guide for Information Security



© 2024

74

74

BAI What to Continuously Monitor

- Local computing environment
- Enclave boundary
- Network and infrastructure
- Supporting infrastructure
- Use a balanced monitoring strategy for subsystems:
 - Do monitor subsystems that did not exist at the beginning of the Software Development Life Cycle SDLC
 - Monitoring continues throughout the Software Development Life Cycle (SDLC)

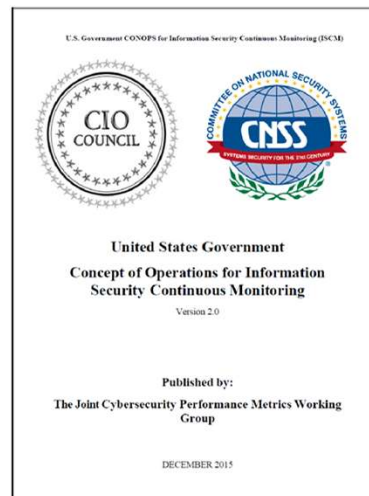
© 2024

75

75

BAI Department of Homeland Security (DHS) CONOPS ISCM Guidance

- DHS Continuous Diagnostics and Mitigation (CDM) Program
- Joint Cybersecurity Performance Metrics Working Group developed CONOPS for ISCM:
 - Supplements NIST guidelines
 - Provides implementation guidance / roadmap for ISCM
 - Applies to non-NSS, NSS and intelligence systems within CNSS jurisdiction
 - Government wide Blanket Purchase Agreement (BPA)
 - Important: Does not apply to DoD NSS—that is DISA responsibility



*REF: United States Government
Concept of Operations (CONOPS)
for Information Security
Continuous Monitoring*

© 2024

76

76

BAI DHS Monitoring Service

- Provided as an example; not targeted to DoD
- DHS Continuous Diagnostics and Mitigation service
- Partnership with the General Services Administration
- Monitoring service for a fee
- CDM blanket purchase agreement (BPA)

<https://www.dhs.gov/cisa/cdm>

DHS CDM Process



© 2024

77

77

BAI ISCM CONOPS Implementation

- To Implement
 - Either: Do it yourself with Commercial Off-the-Shelf (COTS)/Government Off-the-Shelf (GOTS) tools
 - Or: Leverage the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program
- CONOPS Phases "A set of requirements to continuously monitor."
 - Phase 1:
 - Asset management
 - Malware detection
 - Vulnerability management
 - Configuration management

© 2024

78

78

BAI Automated Tools and RMF – Not Just for Monitoring and Assessment

- Developmental testing
- Operations and maintenance
- Troubleshooting
- See NIST SP 800-137, Appendix D, for enabling automation of some ISCM tasks



© 2024

79

79

BAI Building a Continuous Monitoring Strategy

Criticality

- What is the criticality of the security control to maintaining the system's cybersecurity posture?

Frequency

- How often will you monitor this control (i.e., continuous, daily, weekly, bi-weekly, monthly, quarterly, semi-annually, annually)?

Method

- How will you monitor the performance of this control; what is the monitoring activity?

Expected Results

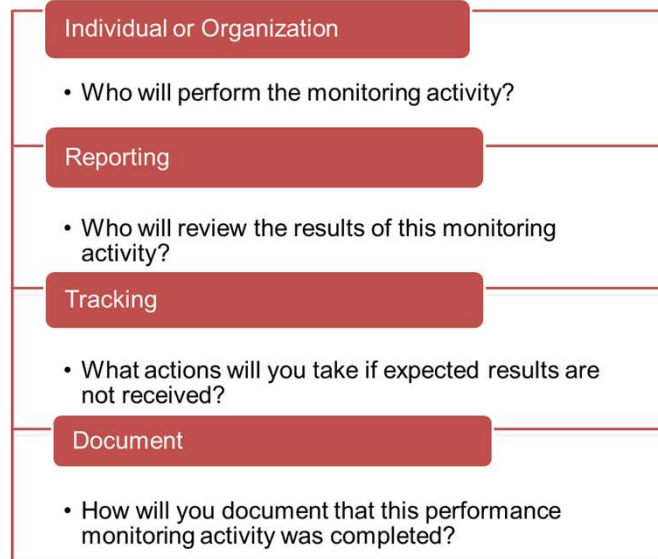
- What do you expect to receive from this monitoring activity?
- Will metrics be used to measure performance?

© 2024

80

80

BAI Building a Continuous Monitoring Strategy



© 2024

81

81

BAI DoD Implementations of Continuous Monitoring Strategy

System-Level Continuous Monitoring Strategy for [System Name]

| Implementation Status / Security Control Status | | | | Continuous Monitoring Strategy | | | | | |
|---|--|-----|----------|--------------------------------|-----------|--------|-----------|----------|----------|
| Security Control Number | Security Control / Enhancement Name | ... | Comments | Criticality | Frequency | Method | Reporting | Tracking | Comments |
| AC-1 | Access Control Policy and Procedures | | | | | | | | |
| AC-2 | Account Management | | | | | | | | |
| AC-2(4) | Account Management Automated Audit Actions | | | | | | | | |

Source: DoD Knowledge Service <https://rmfks.osd.mil>
Help and Resources/References/KS Reference Library

© 2024

82

82

BAI DoD Implementations of Continuous Monitoring Strategy

eMASS System Level Continuous Monitoring

The screenshot shows the 'Edit Implementation Plan' window in the eMASS system. On the left is a sidebar with a search bar and a list of controls. The main panel is divided into two sections: 'Selected Controls (3)' and configuration options. Under 'Selected Controls (3)', there are two status groups: 'Planned (2)' with controls AC-1 and AC-2(6), and 'Implemented (1)' with control AC-2(5). The configuration options on the right include:

- Implementation Status:** Planned (dropdown)
- Security Control Designation:** System-Specific (dropdown)
- Estimated Completion Date:** 18-Dec-2018 (text field)
- Comments:** This is an example comment. (text area)
- Responsible Entities:** Sample responsible entities. (text area)
- System-level Continuous Monitoring (SLCM) Strategy:**
 - Criticality:** Sample Criticality. (text field)
 - Frequency:** Weekly (dropdown)
 - Method:** Manual (dropdown)
 - Reporting:** Sample reporting. (text field)
 - Tracking:** Sample tracking. (text field)
 - SLCM Comments:** Sample comments. (text field)

 At the bottom right are 'Save' and 'Cancel' buttons.

© 2024

83

83

BAI RMF Project Planning

- Major Milestones
 - Identification/Documentation of Common Controls
 - Selection/Documentation of Remaining Controls
 - Overlays
 - Tailor (Scoping Guidance, Compensating, Parameterization)
 - Supplementing
 - Information System Continuous Monitoring Strategy
 - Approved Security Plan
- Primary Roles
 - PM/SM/ISO
 - AO/AODR
 - CIO or SISO
 - Information Security Architect
 - Common Control Provider

© 2024

84

84

BAI RMF Project Planning

- Supporting Roles
 - Risk Executive (function)
 - CIO, SISO, ISSM, ISSO
 - Operational Personnel (administrators, etc.)
- Resources Required
 - Role Holders to Select Controls
 - Qualified Security and Operational Personnel
 - Tool to Document Selected Controls (eMASS, etc.)
- Timeframe
 - Depends on Tailoring and Supplementing Requirements (days to weeks)
 - Developing ISCM may require more time

© 2024

85

85

BAI Guidance and Templates

- NIST SP provide guidance and templates:
 - System Security Plan (NIST SP 800-18)
 - Contingency Plan (NIST SP 800-34)
 - Incident Response Plan (NIST SP 800-61)
 - Security Controls (NIST SP 800-53 Rev 4/5)
 - Configuration Management (NIST SP 800-128)
 - Information System Continuous Monitoring (NIST SP 800-137)

NOTE: Automated tools (e.g., eMASS, Xacta) produce documents in a predefined format

© 2024

86

86

BAI Update System Security Plan

- Critical Artifacts
 - Approved and signed Policy and Procedures for Security controls
 - Risk assessment
 - Privacy impact assessment
 - System interconnection agreements
 - Contingency plan
 - Security configurations for Hardware/software
 - Configuration management plan/process
 - Incident response plan
 - Continuous monitoring plan/strategy

© 2024

87

87

BAI Select Summary Tasks and Responsibilities

| Step 2: SELECT | | |
|---|---|---|
| RMF Tasks | Per DoD KS Primary Responsibility | Per DoD KS Stakeholders |
| Common Control Identification | Common Control Provider (owner) DoD CIO DoD Component CIO Information Security Architect SISO | AO or AODR ISO IS Security Engineer Risk Executive Function |
| Select Security Controls | ISO PM/SM IS Security Engineer | AO or AODR IO ISSM |
| Develop system level continuous monitoring strategy | ISO ISSM SCA PM/SM | AO or AODR Common Control Provider (owner) CIO IO Risk Executive (function) SISO |
| Review and approve the security plan and continuous monitoring strategy | AO or AODR | CIO ISO PM/SM Risk Executive (function) SISO |
| Apply overlays and tailor | ISO PM/SM Systems Security Engineer | AO or AODR IO ISSM |

© 2024

88

88

BAI Select Process Review

- Under what circumstances would you use an overlay?
- What are some examples of currently existing overlays?
- What are some examples in which you would consider scoping considerations?
- In what situations might you need to supplement controls?



© 2024

89

89

BAI Select Process Review

- What are some examples of common controls?
- What are some factors to consider in establishing frequency guidelines for continuous monitoring?
- Provide a situation that could change the monitoring frequency of a control?
- What NIST publication provides guidance on implementing an ISCM?



© 2024

90

90



End of Section 2

NEXT: "Implement"

91