

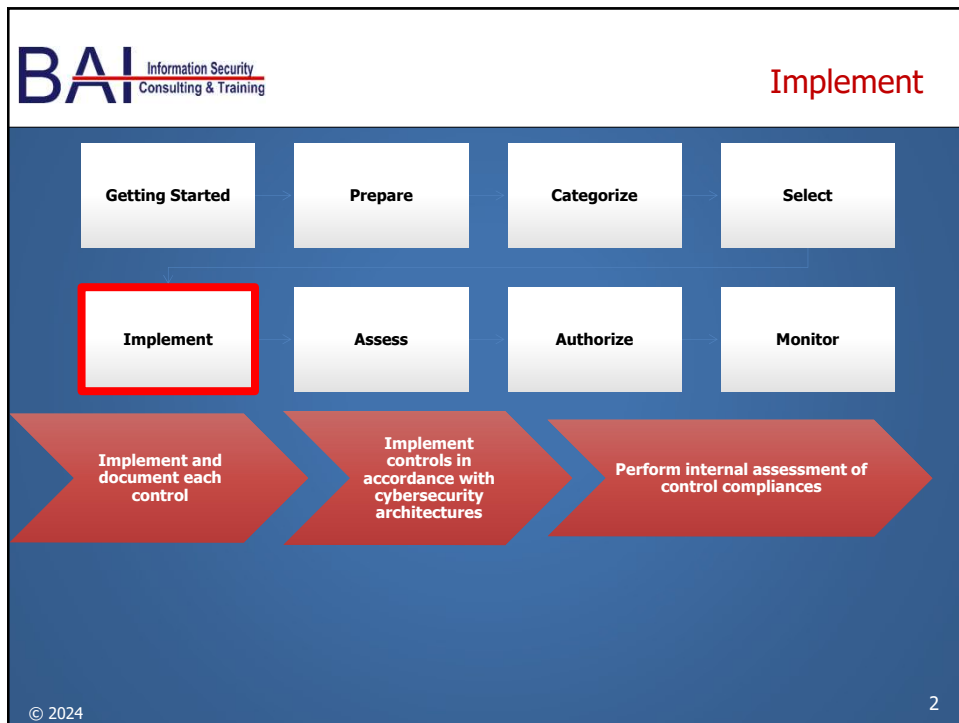


RISK MANAGEMENT FRAMEWORK (RMF) for DoD IT *In Depth* Part 3 v9.0

BAI Information Security
Consulting & Training
© 2024

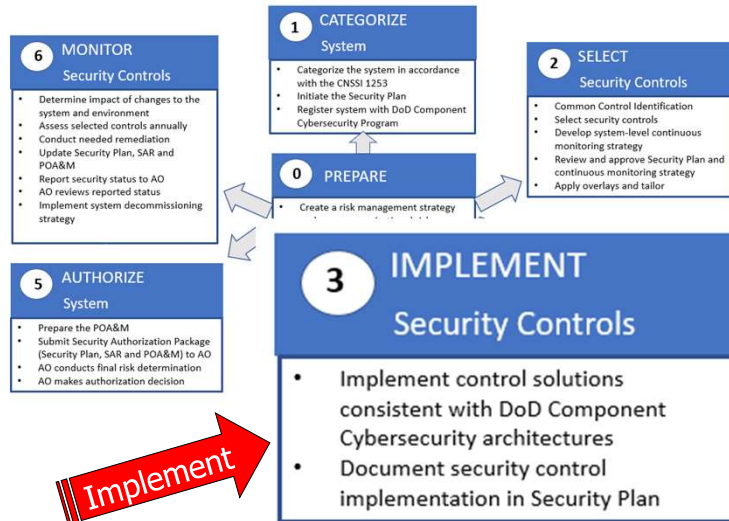
1

1



2

BAI Where We Are In the RMF for DoD Process



© 2024

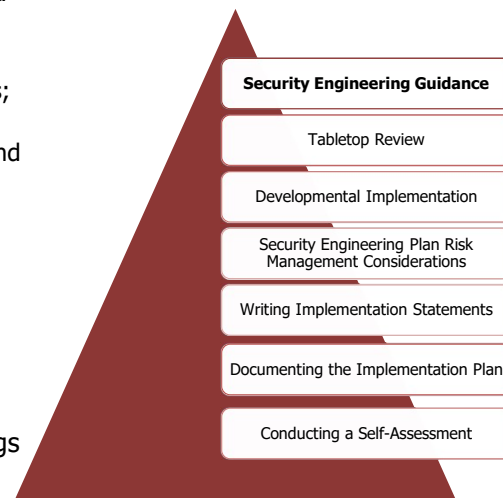
Source: DoD Knowledge Service

3

3

BAI Security Engineering Guidance

- Implement controls using DoD Knowledge Service, Federal and Agency architectures and standards:
 - Security engineering principles;
 - System and software engineering methodologies; and
 - Secure coding techniques;
- System engineering process includes:
 - Describe cybersecurity requirements
 - Identify Risk Management considerations
- Establish and implement mandatory configuration settings



© 2024

4

4

BAI Tabletop Reviews

- Document status of security controls
- Local team conducts internally:
 - Security Team
 - Developers/Engineers
 - Physical Security
 - Personnel Security
- Verifies Common and Not Applicable controls
- Executed within Security Plan
- Identifies additional implementation resources
- Periodic Implementation reviews:
 - Good project management practice
 - Keeps everyone on track
 - Identifies problem areas sooner



© 2024

5

5

BAI Developmental Implementation

- Developmental Implementation assessments ("developmental testing" and "evaluation")
- Conducting security control assessments early:
 - Typically, more cost-effective method to correct
 - Helps identify weaknesses and deficiencies early
- Some artifact requirements are unique to acquisition such as Program Protection Plan (PPP), a milestone acquisition document that covers systems security engineering and security activities as the system continues to be defined.
- See the below link for the Defense Acquisition website.

<https://dau.edu/>




© 2024

6

6

BAI Security Engineering Plan Risk Management Considerations

- Deploy Cross Domain Solution (CDS) on system with higher classification
- Implement Unified Capabilities (UC) products inside authorization boundaries
- Use "Type authorization" to deploy identical copies of an IS or PIT in specified environments
- Standalone systems authorized as any other IS and PIT systems (tailored accordingly)
- Systems operated by a contractor on behalf of DoD (must go through RMF)
 - Explicitly detail responsibilities at the control level
 - Include performance and service-level parameters




© 2024 7

7

BAI Writing Implementation Statements

- Just read the control and say what will you do to implement the requirements stated for the control:
 - Keep it simple and concise.
 - Show it does what is required
 - Who is responsible
 - Give evidence of desired outcomes and how to test, e.g.:
 - Schedule of vulnerability scans
 - Approved policy
 - How an account is set up
 - Automated tools, such as eMASS, have limited space.
 - Plan to reference supporting documentation.



© 2024 8

8

BAI Example Implementation Statement

- PE-2 PHYSICAL ACCESS AUTHORIZATIONS
 - Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
 - Issue authorization credentials for facility access;
 - Review the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*];
 - Remove individuals from the facility access list when access is no longer required.
- PE-2 Example Implementation Statement
 - A list of individuals with authorized access to the XYZ facility has been created and is maintained by the ISSO. The System Owner approves the list of authorized individuals.
 - The XYZ facility Physical Security Division updates the Agency CAC with authorized individual access information contained on the System Access Authorization Request (SAAR) form that is signed by the individual's supervisor and the ISSO.
 - The XYZ facility Physical Security Division, ISSO, and everyone's supervisor, reviews the access list quarterly.
 - When notified by an individual's supervisor, the ISSO removes an individual's name from the facility access list when access is no longer required and notifies the XYZ facility Physical Security Division to remove the associated individual's CAC authorizations.

© 2024

9

9

BAI Documenting the Implementation Plan

- Who has contributed
- Provides an overview of the system security requirements
- Describes controls as "in place" or "planned" or "implemented"
- Delineates responsibilities of those with system access
- Common controls are identified
- Hosting system provides compliance status
- Reference functional specifications and security-relevant documentation to help increase efficiency (vendor, systems integrators, etc.)
- Keep it accurate and real! Perfection is rarely achievable!



© 2024

10

10

BAI Conducting a Self-Assessment

- Conduct a complete internal review prior to formal security control assessment
- Examine, Interview, Test
- How will you test that the system meets the requirements? E.g.
 - Look at group policy objects.
 - Act as a user and create a password that does not meet the requirement.
- Use same tools the assessor will be using to execute automated scans
- Review security control artifacts
- Interview responsible individuals
- Document results

Security Engineering Guidance

Tabletop Review

Developmental Implementation

Security Engineering Plan Risk Management Considerations

Writing Implementation Statements

Documenting the Implementation Plan

Conducting a Self-Assessment

© 2024

11

11

eMASS Control Implementation Plan

Authorization		Assigned Security Controls					Edit Selected Cancel	
Search:		Control Acronym	Implementation Status	Security Control Designation	Responsible Entities	Estimated Completion	Select Visible	
Controls Controls Listing Implementation Plan Risk Assessment Import/Export Bulk Processing Assets Actions Findings Resources HW Baseline SW Baseline Ports/Protocols Import/Export		AC-1	Planned	Hybrid	Sample Responsible Entities.	30-Apr-2018	<input checked="" type="checkbox"/>	
		AC-2	Inherited	Common	eMASS Training System: Sample Responsible Entities.	31-May-2016		
		AC-2(1)	Inherited	Hybrid	Sample Responsible Entities.	05-Jan-2016		
		AC-2(2)	Inherited	Common	Sample Responsible Entities.	31-May-2016		
		AC-2(3)	Inherited			31-May-2016		
		AC-2(4)	Inherited		To be determined.	31-May-2016		
		AC-2(5)	Implemented	System-Specific	Individuals responsible for implementing this Control.	17-Apr-2018	<input checked="" type="checkbox"/>	
		AC-2(6)	Planned	System-Specific	Application support team is responsible for this Control.	30-Apr-2018	<input checked="" type="checkbox"/>	

© 2024

12

12

eMASS Control Implementation Plan

Controls
 Controls Listing
Implementation Plan
 Risk Assessment
 Import/Export
 Bulk Processing

Assets
 Actions
 Findings
 Resources
 HW Baseline
 SW Baseline
 Ports/Protocols
 Import/Export

POA&M
 POA&M Listing
 POA&M Import
 POA&M Export

Artifacts
 Artifact Listing

Reports
 System Reports

Workflows
 Active Workflow Listing
 Historical Workflow Listing

Relationships
 Inheritance
 Associations
 Inheritability
 Requests & Approvals

Management
 Personnel
 Workload Tasks
 Administration

Edit Implementation Plan

Selected Controls (1)
Status
 Planned (1)
 AC-1

Implementation Status:
 Security Control Designation:
 Test Method:
 Estimated Completion Date:
 Implementation Narrative:
 Responsible Entities:

System-level Continuous Monitoring (SLCM) Strategy
 Criticality:
 Frequency:
 Method:
 Reporting:
 Tracking:
 SLCM Comments:

13

13

- BAI** **RMF Controls and Automation:**
CM-6 Configuration Settings
- Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];
 - Implement the configuration settings;
 - Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
 - Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
- (1) CONFIGURATION SETTINGS | AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION**
Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].

© 2024

14

14



RMF Controls and Automation: RA-5 Vulnerability Monitoring and Scanning

- a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
- b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 1. Enumerating platforms, software flaws, and improper configurations;
 2. Formatting checklists and test procedures; and
 3. Measuring vulnerability impact;
- c. Analyze vulnerability scan reports and results from vulnerability monitoring;
- d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;
- e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems.

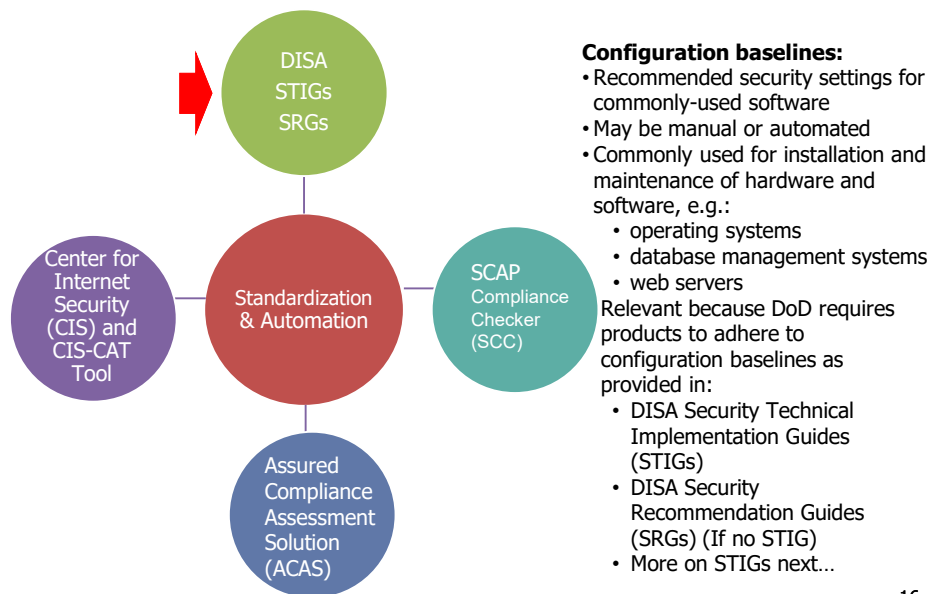
© 2024

15

15



Security Configuration Tools



© 2024

16

16



What are STIGs?

Configuration standards for DOD IA and IA-enabled devices/systems.

Contains technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

Most STIGs are created by vendors based on a technology's DoD SRG (Security Requirements Guide).

STIGs are generally updated on a quarterly basis.

© 2024

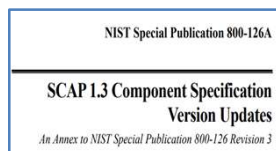
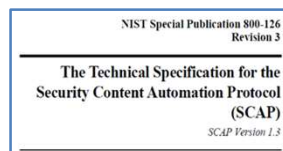
17

17



Security Configuration Tools

- DISA Security Technical Implementation Guides (STIGS)
 - Available on the Cyber Exchange website <https://cyber.mil> or <https://public.cyber.mil>
- SCAP - Security Content Automation Protocol (SCAP) is standardized content for use with a tool to express security flaws and establish configuration settings. SCAP is the protocol; STIG is the checklist.
- SCAP uses specific standards to enable automation for:
 - Vulnerability management
 - Policy compliance evaluation (e.g., FISMA compliance)
 - Automated tools help validate STIG compliance
 - Only some STIG items can be automatically verified.
 - Some items will always need to be checked manually.



© 2024

18

18

BAI Technologies Covered by STIGS

The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

A STIG describes how to minimize network-based attacks and prevent system access when the attacker is interfacing with the system, either physically at the machine, or over a network.

STIGs also describe maintenance processes, such as software updates and vulnerability patching.

Some controls require a checklist to verify configuration.

OPERATING SYSTEMS

Windows
Mainframe
Unix/Linux
Virtualization
MAC OS
General Purpose
Cross Domain Solutions

NETWORK/PERIMETER/ WIRELESS

Network Infrastructure
Telecommunications
Enclave and DMZs
Backbone Transport
Cloud Security

APPLICATION SECURITY

Application Servers
Application Services
Browser Guidance
Database
Desktop
Office Automation
Remote Desktop
Web Servers

MOBILITY

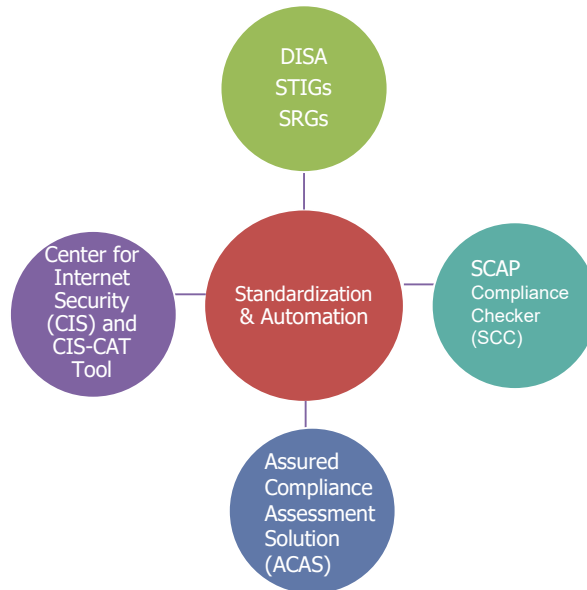
Smartphones
Tablets

© 2024

19

19

BAI Security Configuration Tools



Two major automated tools that you need to know. First:

- SCAP Compliance Checker (SCC) - checks for STIG compliance (per configuration baselines)

© 2024

20

20

BAI SCAP Compliance Checker (SCC)

- SCC is a STIG scanning software that validates configuration - automates assessment of STIG compliance
-
- DISA maintains the authoritative download of SCC, and starting with SCC 5.4, no longer requires a CAC to download
- DISA provides the standard SCAP benchmark files that include rules that can be verified automatically
 - <https://public.cyber.mil/stigs/scap>
- Naval Information Warfare Center includes enhanced content that allows you to answer manual questions and create the STIG checklist file right from the SCC application.
 - <https://niwcatlantic.navy.mil/scap/scap-content-repository/>

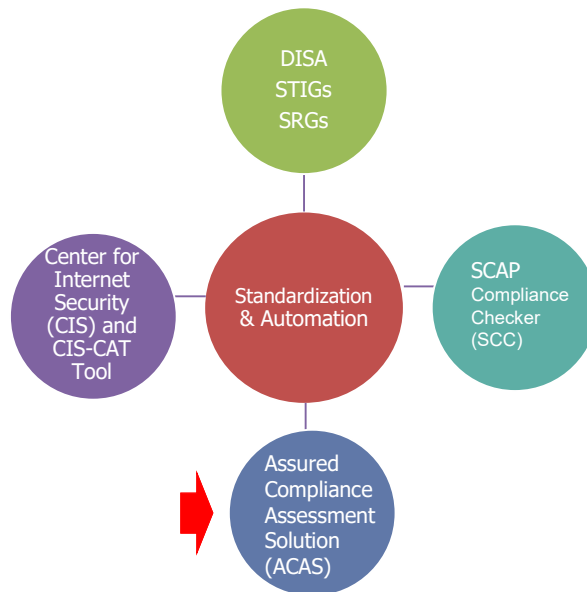


© 2024

21

21

BAI Security Configuration Tools



Second of two major automated tools that you need to know:

DISA Assured Compliance Assessment Solution (ACAS) standard vulnerability scanner

© 2024

22

22

BAI DISA Assured Compliance Assessment Solution (ACAS)

- **NESSUS Security Center:** Central console for vulnerability and compliance scanning.
- **NESSUS User Interface:** A fully capable scanner covers a breadth of checks, including unique Common Vulnerabilities and Exposures (CVEs), and successfully operates across different environments.
- Tenable's Unified Security Monitoring platform is the U.S. Defense Information Systems Agency (DISA) vulnerability management solution deployed DoD-wide as the **Assured Compliance Assessment Solution (ACAS)**.
- The ACAS Security Center central console automates and can scale to an organization's vulnerability and compliance scanning infrastructure. It also can provide capabilities to allow for management, alerting, and reporting against vulnerability and compliance requirements.

ACAS COMPONENTS

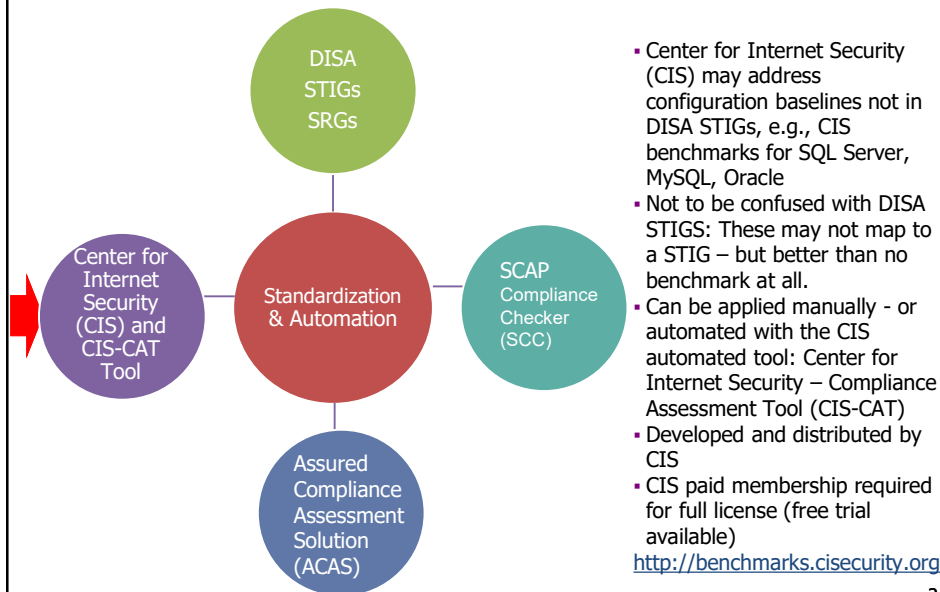


© 2024

23

23

BAI Security Configuration Tools



- Center for Internet Security (CIS) may address configuration baselines not in DISA STIGs, e.g., CIS benchmarks for SQL Server, MySQL, Oracle
- Not to be confused with DISA STIGs: These may not map to a STIG – but better than no benchmark at all.
- Can be applied manually - or automated with the CIS automated tool: Center for Internet Security – Compliance Assessment Tool (CIS-CAT)
- Developed and distributed by CIS
- CIS paid membership required for full license (free trial available)

<http://benchmarks.cisecurity.org>

© 2024

24

24



DISA Continuous Monitoring and Risk Scoring Tool (CMRS)

- DoD web application cybersecurity risk monitoring/ reporting
 - Controls that rely on automated tools
 - Software inventory
 - AV configuration
 - STIG compliance
 - IAVM (vulnerability & patch compliance)
- Dashboards display quantitative security posture based on ESS (Endpoint Security Solutions) and ACAS data



FYI only. CMRS may not be in common use

© 2024

25

25



Security Tools for IS Professionals

- Understand what tools do and how to use them:
 - Some need to be run during non-working hours
 - Test tools before running on operational network
 - Training is essential
- SecTools.org: Catalog and great information about various security tools
- Beware! Scanning tools can cause:
 - Certain types of scanning activity may be prohibited on government networks without explicit permission
 - Network performance degradation
 - Outright failure (crashes) of operating systems or applications



© 2024

Security Tools Website: <http://sectools.org>

26

26

BAI RMF Project Planning

- Resources Required
 - Qualified Security and Operational Personnel to Implement and Document Selected Controls
 - Involve qualified IS security engineers early.
 - Tool(s) to Document Implemented Controls (eMASS, etc.)
- Timeframe
 - Weeks to Months dependent on Implementation and System Development Requirements & Timelines

© 2024

27

27

BAI Select and Implementation Results/Artifacts

- System Baseline (list of controls based on C, I, A)
 - include CCIs
- Common Control List – Inherited and Common Policy (Contract, MOA, MOU, SLA)
- Security Control Implementation Plan
- Security Control Policy/Procedures
- Test Results (i.e., CCI self-assessments)
- Contingency Plan/Disaster Recovery
- Configuration Management Plan/CCB Charter
- System Interconnection Agreements
- System Security Configuration Documents
- Incident Response Plan



© 2024

28

28

BAI Implement Summary Tasks and Responsibilities

Step 3: IMPLEMENT SECURITY CONTROLS		
RMF Tasks	Per DoD KS Primary Responsibility	Per DoD KS Stakeholders
Implement control solutions consistent with DoD Component Cybersecurity architectures	ISO PM/SM System Security Engineer	Common Control Provider (Owner) IO ISSM
Document security controls implementation in the security plan	ISO PM/SM	Common Control Provider (Owner) IO ISSM System Security Engineer

© 2024

29

29

BAI Review

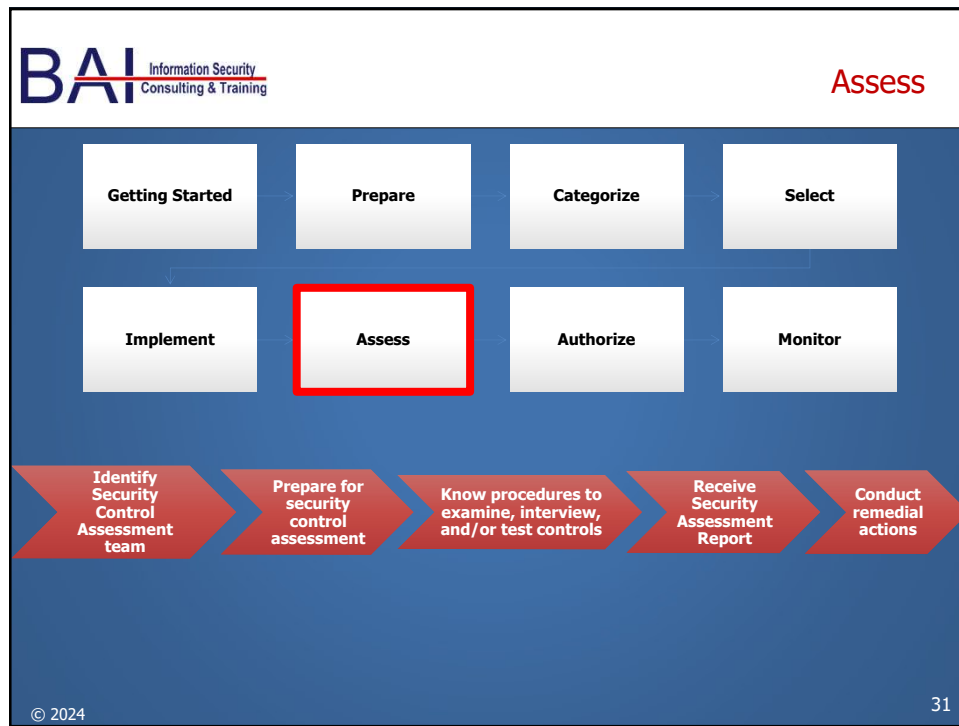
- What are examples of when you might need to use standardized configurations (e.g., STIG, CIS Benchmarks, etc.)?
- How do you think of standardized configurations in relation to SCAP?
- How might various automated tools support RMF?
- How does standardization support information security?



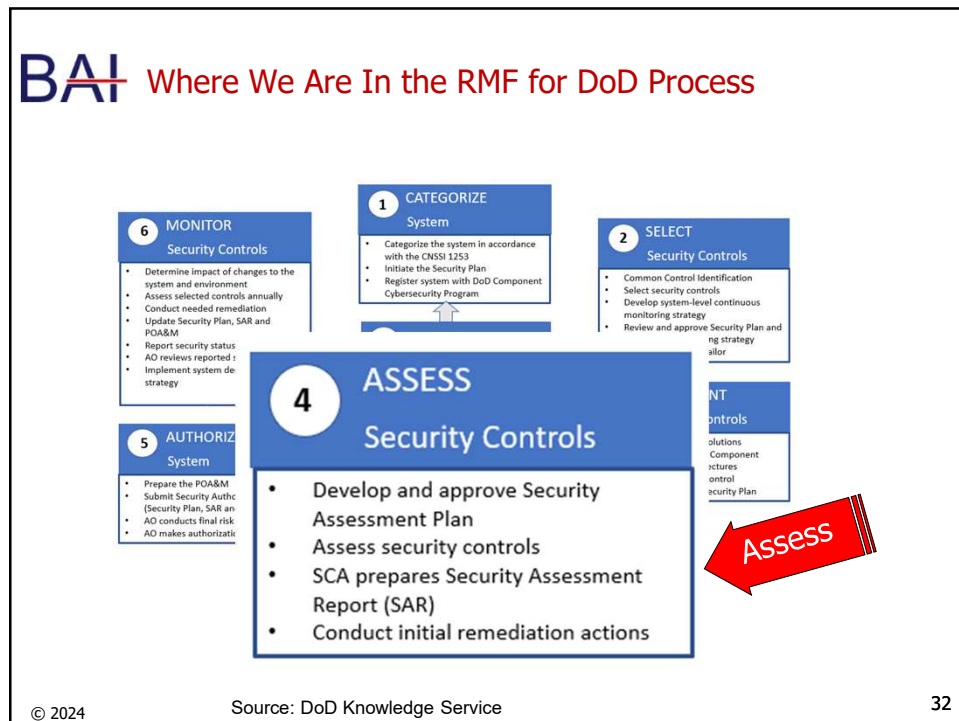
© 2024

30

30



31



32

BAI Security Assessment Plan

- Defines type of assessment and procedures
- Determines extent control requirements are met:
 - Correctly implemented?
 - Operating as intended?
 - Producing desired outcome?
- SCA develops plan
 - Identifies assessors
 - Ensures activities are documented in:
 - the security assessment plan and
 - the program T&E (test and evaluation) documentation
 - Helps maximize effectiveness, reuse, and efficiency
- Assessment methods: Examine, Interview, Test

© 2024

33

33

BAI Security Control Assessor - Qualifications

- SCA must be qualified to:
 - Follow security assessment plan to assess stated procedures
 - Provide specific recommendations on how to correct weaknesses/deficiencies to reduce or eliminate vulnerabilities:
 - Use technical skills to evaluate system-specific, hybrid, and common controls, including:
 - Hardware, software, and firmware knowledge
- Independent – no conflict of interest regarding:
 - IS development, operation, and/or management

© 2024

34

34

BAI Assessment Procedures

- Assessment objectives:
 - Contain associated methods and objects
 - Includes determination statements specific to the control
- Attributes to look for:
 - Depth (Basic, Focused, Comprehensive)
 - Coverage (Basic, Focused, Comprehensive)
 - Determined by Assurance Requirements
 - Defined by Organization
- Assess, document and record compliance results per relevant:
 - Configuration standards (e.g., STIG, SRG, Benchmarks, etc.)
 - Agency Guidance

© 2024

35

35

BAI Assessment Plan – Example Items

- | | |
|---|---|
| <ul style="list-style-type: none"> ■ Scope: System Name/Title ■ What will be tested, e.g.: <ul style="list-style-type: none"> ■ IP Addresses ■ Web Applications ■ Databases ■ Roles Slated ■ Assumptions <ul style="list-style-type: none"> ■ System access ■ Employee availability ■ Hours | <ul style="list-style-type: none"> ■ Methodology <ul style="list-style-type: none"> ■ Documentation to be reviewed, travel ■ Test plan, e.g. <ul style="list-style-type: none"> ■ Assessment Team ■ Automated Tools ■ Manual Methods ■ Rules of engagement ■ Disclosures ■ Security testing inclusions/exclusions ■ How test results will be communicated |
|---|---|

© 2024

36

36

BAI Assessment Procedures Example CP-2 (800-53A R5)

- CP-02(a)(01) "A contingency plan for the system is developed that identifies essential mission and business functions and associated contingency requirements."



EXAMINE Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; evidence of contingency plan reviews and updates; system security plan; other relevant documents or records.



INTERVIEW Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities.



TEST Organizational processes for contingency plan development, review, update, and protection; mechanisms for developing, reviewing, updating, and/or protecting the contingency plan.

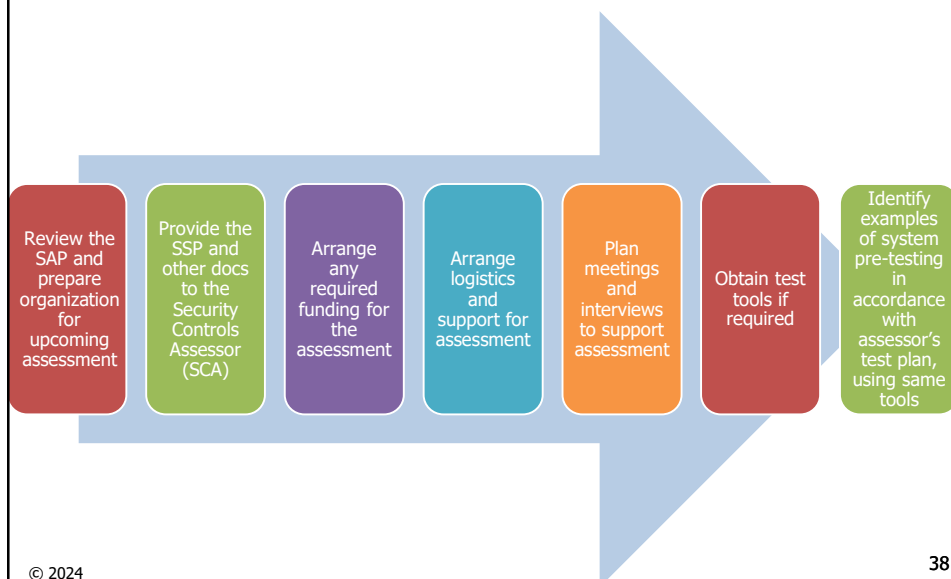
© 2024



37

37

BAI Organization Preparation for the Assessment



© 2024

38

38

BAI Incremental Assessment(s)

- Controls that may be assessed prior to all controls being fully implemented
- Examples
 - Policy, procedures, and plans assessed prior to hardware/software technical security controls
 - Common controls (i.e., security controls inherited by the information system) assessed prior to the system security controls
 - Site Assistance Visits from organizational personnel

© 2024

39

39

BAI Self-Assessment Techniques

- Techniques for control self-assessment:
 - Internal Control Questionnaire (ICQ) self-audit
 - Customized questionnaires
 - Control guides
 - Interviews
- In DoD, system owners ensure that all Control Correlation Identifiers (CCIs) are completed via self-assessment prior to the Independent Assessment

© 2024

40

40

BAI Existing Assessment(s)

- SCAs will maximize reuse of existing assessment (i.e., a leveraged authorization, Type Authorization) and T&E documentation
- Greatest potential for reuse:
 - Type Authorization: Single package for identical copies of system deployed in different environments.
 - Leveraged authorization: reuse of an existing authorization from another system, e.g., another federal agency or DoD component, or a commercial entity authorized by the government such as the cloud

© 2024

41

41

BAI Assessments of External Provider Controls

- When controls are provided by an external provider, the organization ensures assessors have:
 - access to the information system and environment of operation where the controls are employed
 - appropriate information needed in order to carry out the assessment
- If possible, provide/reuse existing assessments conducted by the external provider

© 2024

42

42

BAI eMASS Control Details -> Assessment Procedure

AC-1	NCUO	Access Control Policy And Procedures	B	Moderate
AC-2	NCUO	Account Management	B	Moderate
AC-2(1)	CUO	Automated System Account Management	B	Low
... AC-2(1).1	C	CCI: 000015		

From the "Controls/Listing" view, expand the desired Security Control and click on the hyperlinked Assessment Procedure

Test Result History						
Entries Showing 10						
Status	Test Date	Tested By	Test Results	Type	Created By	Created Date
Compliant	11-Apr-2022	John Smith	Additional Compliant Test Result.	Validation	Smith, John (CTR; DoD)	11-Apr-2022
Compliant	11-Apr-2022	John Smith	Compliant Test Result.	Self-Assessment	Smith, John (CTR; DoD)	11-Apr-2022

A history of all the Test Results entered for a given AP are displayed at the bottom of "Assessment Procedure Details" page.

© 2024

43

43

BAI Control Correlation Identifier (CCI)

Basic element of IA policy or standard:

- Deconstructs NIST SP 800-53 R5 IA Controls or IA industry best practices into single, actionable statements
- Written neutrally so not to imply requirement specifics.
- Not specific to a product or a Common Platform Enumeration (CPE).

Enables tracing of security requirements:

- From origin (e.g. regulations, IA frameworks) to their low-level implementation.
- Links requirements to policy – reduces ambiguity
- Allows organizations to demonstrate compliance to multiple IA compliance frameworks.
- Provides a way to objectively rollup and related compliance assessment results across disparate technologies.

CCI List:

- Collection of CCI Items, which express common IA practices or controls at the federal level

CCI data specification:

- Proposed to work with NIST Security Content Automation Protocol (SCAP)
- Should not require changes to SCAP tools

© 2024

44

BAI Control Correlation Identifier (CCI) – Example from the Knowledge Service

Control Number	800-53 Control Text Indicator	CCI	CCI Definition	Implementation Guidance	Assessment Procedures
IR-8	IR-8 (c)	CCI-000847	The organization defines the frequency for reviewing the incident response plan.	DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	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 at least annually (incorporating lessons learned from past incidents).
IR-8	IR-8 (c)	CCI-000848	The organization reviews the incident response plan on an organization-defined frequency.	The organization being inspected/assessed will conduct reviews of its incident response plan at least annually. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).	The organization conducting the inspection/assessment obtains and examines the incident response plan to validate it is current and has been reviewed within the last year. DoD has defined the frequency as at least annually (incorporating lessons learned from past incidents).
IR-8	IR-8 (d)	CCI-000849	The organization updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	The organization being inspected/assessed must update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporate lessons learned from past incidents (IR-4a). The organization must document the	The organization conducting the inspection/assessment obtains and examines documentation of the update actions for the incident response plan to ensure the organization is updating the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporating lessons learned from past incidents (IR-4a).

© 2024

45

45

BAI Security Assessment Report (SAR)

- Communicates risk posture
- Provides a disciplined method to identify/mitigate risk
- Documented with detail appropriate to assessment
 - Type of assessment (e.g., self-assessments, audits)
 - In accordance with reporting format prescribed by organizational and/or federal policies
 - Recommendations to correct weaknesses and deficiencies
 - Areas for further investigation
- Executive summary:
 - Synopsis of assessment
 - Key findings
 - Recommendations for addressing security control weaknesses and deficiencies

© 2024

46

46

BAI Creating the POA&M

- Identifies residual vulnerabilities, weaknesses, deficiencies
 - Defines resources (personnel, funding, etc.) to accomplish tasks
 - Establishes schedule and milestones in meeting the tasks
 - Weaknesses should be traceable to one or more controls
 - Controls are no longer considered Implemented
 - Provide supporting evidence as Planned or In-Place
 - POA&M detail at control level and possibly CCI level
-
- Follow organization or agency guidance, i.e., utilize templates, automated tools, etc.

© 2024

47

47

BAI eMASS – POAM Item

The screenshot displays the eMASS POAM Item interface. On the left is a navigation menu with options like Assets, Actions, Findings, Resources, HW Baseline, SW Baseline, Ports/Protocols, Import/Export, POA&M (selected), POA&M Listing, POA&M Import, POA&M Export, Artifacts, Artifact Listing, Reports, System Reports, and Workflows. The main area is titled 'POA&M Items for Controls, APIs, and System' and includes a 'POA&M Item Actions' dropdown. Below this are 'Table View' and 'Card View' tabs. A table lists POAM items with columns for ID, Control / AP, Severity, Residual Risk Level, View / Edit Vulnerability Description, Created Date, Scheduled Completion Date, Status, Review Status, and Select. The table shows four items with varying severity levels (Very Low, Moderate) and statuses (Completed, Ongoing, Not Applicable).

ID	Control / AP	Severity	Residual Risk Level	View / Edit Vulnerability Description	Created Date	Scheduled Completion Date	Status	Review Status	Select
101750014	System	Very Low	Very Low (Recommended Very Low)	View Description	12-Apr-2022	12-Apr-2022	Completed	Approved	<input type="checkbox"/>
101750015	System	Moderate	Moderate (Recommended Moderate)	View Description	12-Apr-2022	30-Sep-2022	Ongoing	Approved	<input type="checkbox"/>
101750013	CAL-3 CUI	Moderate	Moderate (Recommended Moderate)	View Description SV 2903874802715.pdf SV 290394802775.pdf	11-Apr-2022	30-Sep-2022	Ongoing	Approved	<input type="checkbox"/>
101750021	206-3	None	- (Recommended None)	View Description Not Available	13-Apr-2022		Not Applicable	Approved	<input type="checkbox"/>

© 2024

- List is available here of any existing POA&M Items

48

48

BAI Reassessments

- Mitigate weaknesses and deficiencies, then reassess:
 - Implemented correctly?
 - Operating as intended?
 - Producing the desired outcome?
- After assessment, Security Plan updates include:
 - Implemented controls
 - Residual vulnerabilities
- SCA updates findings in Security Assessment Report
- Original Security Assessment Report findings do not change

© 2024

49

49

BAI eMASS Security Assessment Report (SAR)

DoD RMF Security Assessment Report (SAR)

SYSTEM INFORMATION			
System Name (1):		Security Controls Assessor (SCA) and/or SCA Rep (7):	
Example Information System		Smith, John	
System Acronym (2):	Example Information System		
Version / Release Number:	1.X		
System Identification (4):	138	Assessment Completion Date (8):	23 Oct 2018
DoD Component (3):	OSD	Authorizing Official (6):	Package Under Review
System Type (5):	IS Major Application		
		Security Categorization (10):	
		Confidentiality:	Low
Last Updated (8):	23 Oct 2018	Integrity:	High
Information System Owner (11):	DCD	Availability:	Low
Package Type:	Assess and Authorize	Impact:	High
Security Controls Assessor Executive Summary (1):			

After reviewing all of the information, this System's risk is deemed as MODERATE until the identified deficiencies are corrected.

© 2024

50

50

BAI Issue Resolution

Resolution Process

- SCA prepares Security Assessment Report (SAR)
- Identifies actions to address:
 - Non-compliant controls
 - Vulnerabilities
 - Associated risk
- Helps identify false positives
- Shares security status with authorizing officials
- Limits POAM to non-compliant and not applicable items
- System Owner/PM responsible for POA&M
- Communication between AO or AODR and System Owner/PM to discuss POA&M items

© 2024

51

51

BAI Arranging for Assessment

- Processes vary agency to agency
- Have organization officials review/approve to ensure:
 - consistency with organization security objectives
 - that appropriate effort, funding, and resources are applied
- Allocate assessment budget during planning
- Determine whether agency has list of "approved" assessors - make contact early
- Prepare SCA access to:
 - Information system and environment of operations
 - Documentation, records, artifacts, test results, personnel, etc.

© 2024

52

52

BAI Assess Milestones and Primary Roles

- Major Milestones
 - Completed Control Assessment Plan
 - Final Security Control Assessment Report
 - Initial Remediation Actions Completed
- Primary Roles
 - Security Control Assessor
 - PM/SM/ISO
 - Common Control Provider

© 2024

53

53

BAI Assess Planning Resources and Timeframe

- Resources Required
 - Qualified Security Control Assessor Personnel to:
 - Perform Assessment
 - Develop Assessment Report
 - Qualified Security and Operational Personnel to Perform Initial Remediation Actions
 - Tool to Document Assessment and Remediation Actions (eMASS, etc.)
- Timeframe
 - Weeks to Months dependent on Size and Complexity of the System and associated Assessment Procedures

© 2024

54

54



Summary Tasks and Responsibilities

Review with KS updates

Step 4: ASSESS SECURITY CONTROLS			
RMF Tasks	Per DoD KS Primary Responsibility	Per DoD KS Stakeholders	
Develop and approve Security Assessment Plan	AO or AODR SCA	CIO Common Control Provider (Owner) IO	ISO ISSM PM/SM SISO
Assess security controls	Security Control Assessor	Common Control Provider (Owner) IO	ISO ISSM
SCA Prepares Security Assessment Report (SAR)	SCA	Common Control Provider (Owner) ISO ISSM	
Conduct initial remediation actions	ISO PM/SM	AO or AODR CIO Common Control Provider (Owner) IO	ISSM SCA SISO System Security Engineer

© 2024

55

55



Course Activity

- Refer to Course Guide for "Implementation/Assessment/Continuous Monitoring Activity."



© 2024

56

56

BAI Review

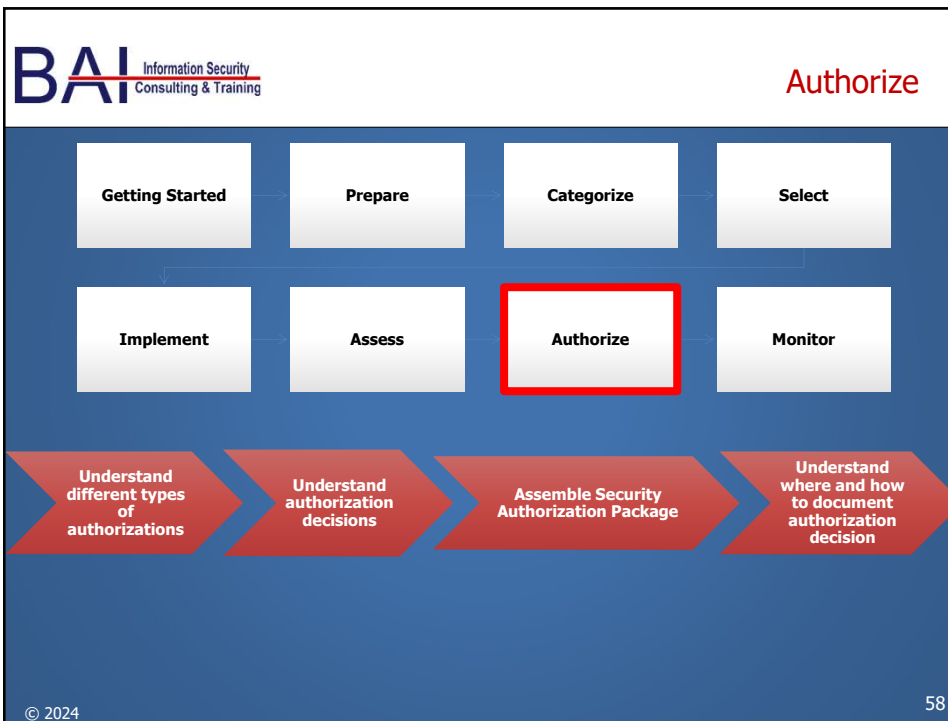
- What are the different methods of assessment?
- How might they be supported with automated tools?
- What are reasons for, or types of, assessments?
- How might you schedule them on a project plan?



© 2024

57

57

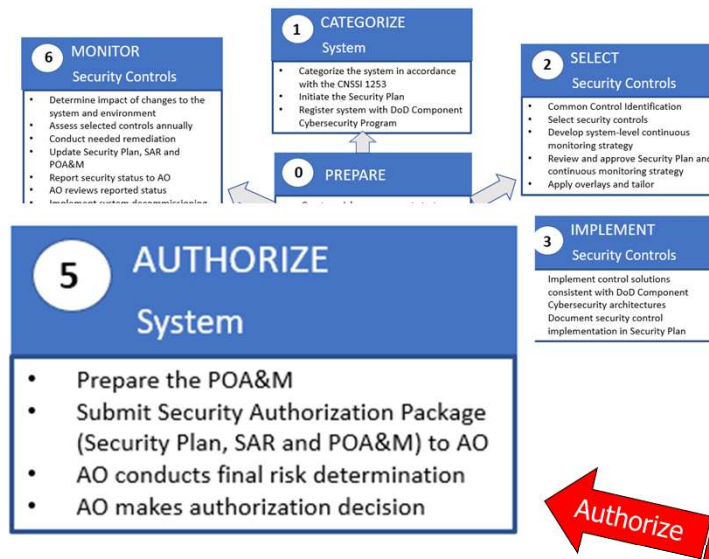


58

58



Where We Are In the RMF for DoD Process



© 2024

Source: DoD Knowledge Service

59

59



POA&M

- Vulnerabilities reporting:
 - Contains vulnerabilities identified during security control assessment
 - Addresses inherited vulnerabilities
 - Once posted, vulnerabilities are updated, but not removed
 - Identifies tasks to remediate/mitigate vulnerabilities
 - Kept active to address vulnerabilities throughout a system's life cycle
- Planning:
 - Specifies resources required
 - Includes schedule and milestones
 - Must be tracked and reviewed
 - Responsibility of System Owner/PM

© 2024

60

60

BAI Authorize Considerations

- Prior to decision - AO collaborates with SISO to assess information, e.g.
 - How organization assesses risk:
 - for known aggregated risks
 - methodologies, techniques, procedures, tools
 - organizational risk mitigation approach/tolerance
 - Mission and operational security requirements
 - Contents of security authorization package
 - Dependencies among information systems
- AO cannot delegate explicit acceptance of risk

© 2024

61

61

BAI Authorization Decisions

- RMF
Authorization
decision options

ATO

- No change

ATO with Conditions

- Replaced "IATO"

IATT

- No change

DATO

- No change

© 2024

62

62

BAI Authorization to Operate (ATO)

- AO issues an ATO when risk is deemed acceptable to:
 - organizational operations and assets
 - individuals
 - other organizations
 - the Nation

© 2024

63

63

BAI ATO with Conditions

- ATO with conditions
- Granted when mission requires the IS to operate despite risks
- ATO establishes terms and conditions
 - Work continues to minimize deficiencies
- ATO with conditions duration typically less than ATO maximum (typically <6 months)
- System owner must continue work on risk mitigation
- Goal is to sufficiently mitigate risk to achieve ATO

© 2024

64

64

BAI Interim Authorization to Test (IATT)

- Special type of authorization decision
- Allows IS test utilizing actual operational/live data for a specified time (usually <90 days)
- AO grants IATT only when live data/operational environment is required to complete specific test objectives
- ISO must present AO with a credible test plan and schedule

Very unique. Check with your AO or AODR on their IATT process and requirements.

© 2024

65

65

BAI Denial of Authorization to Operate (DATO)

- DATO issued when:
 - AO deems risk(s) unacceptable
 - No immediate steps can be taken to reduce to acceptable level
- If system is in operation, all activity is halted.
- Network connections to be terminated immediately.

© 2024

66

66

BAI Ongoing Authorization

- Not yet a reality - more of a long-term goal to:
 - Maintain knowledge of current security state
- Process would involve re-executing RMF step(s)
- Requires maximize use of status reports
- Reauthorization could be:
 - Time-driven
 - Event-driven
- Continuous Monitoring maintains the Assurance Case

© 2024

67

67

BAI Type Authorization

- Single package for identical copies of an IS or subsystem deployed in different environments
- Typically includes:
 - Set of installation guides
 - Configuration requirements
 - Operational security requirements guides
 - Guides are for hosting location use
 - Applied in specified environments of operation. Includes:
 - Hardware
 - Software
 - Firmware
 - and/or applications

© 2024

68

68

BAI Reciprocity

- Defines a streamlined process for acceptance of any authorized system 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 system's security posture
 - Documents acceptance by the receiving AO
 - Updates its authorization to show inclusion of the deployed system

© 2024

69

69

BAI Authorization

- AO establishes Authorization Termination Date (ATD) to indicate authorization expiration/reauthorization timing
- Possible rescission at any time for violations
 - Federal/organizational policies, directives, regulations, standards, guidance, or practice
 - Original authorization terms/conditions
- AO may conduct continuous monitoring review for:
 - risk determination
 - effectiveness of system security controls
- AO may eliminate ATD based on continuous monitoring program success – ongoing authorization

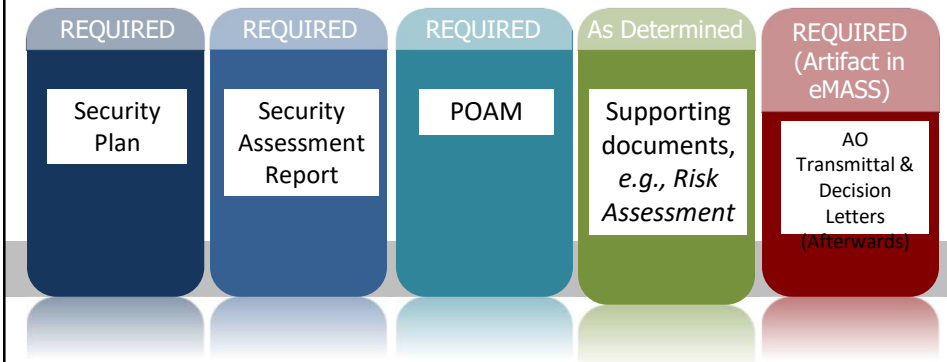
© 2024

70

70

BAI Security Authorization Package

- AO uses Security Authorization package to make risk-based decisions
- May request additional documentation



© 2024

71

71

BAI Security Assessment Report (SAR) to Risk Assessment Report (RAR)

- Risk Assessment Report (RAR):
 - Is now required by CNSSI 1254 (NSS) as part of the authorization package
 - Is a useful tool for communicating risk priorities to Information System Owner
 - RAR is long-term throughout system lifecycle
 - Is useful for determining Continuous Monitoring control strategy and frequencies
 - Security Assessment Report (SAR) can feed the RAR
 - Communicate risk assessment results for controls SAR has identified as non-compliant

© 2024

72

72

BAI eMASS – Creating a New Workflow

Assess and Authorize
Submit a package for an Assessment and Authorization Decision.

Extension
Submit a package for an Authorization Extension.

Interim Authority to Test (IATT)
Initiate a workflow to conduct assessment and authorization activities to achieve an Interim Authority to Test (IATT).

Denial of Authorization to Operate (DAOT)
Submit a package for a Denial of Authorization to Operate Decision (DAOT).

Decommission
Submit a package for a Decommission Decision.

Annual Security Review
Submit one or many Security Controls for review in accordance with annual assessment requirements.

Change Request
Submit a package for the review and approval of a Change Request.

POA&M Approval
Submit one or many POA&M items for approval.

POA&M Quarterly Review
Initiate a workflow to satisfy quarterly Ongoing and Risk Accepted POA&M review requirements.

Risk Acceptance Approval
Submit one or many Risk Accepted POA&M items for approval.

Security Plan Approval
Submit the system's Security Plan Report for AO approval.

© 2024 73

73

BAI eMASS – Creating a New Workflow

Create New Assess and Authorize

Rules: AO, C&A Team, PM&AM, SCA

0 days Incomplete 1. PM&AM

0 days Incomplete 2. C&A Team

0 days Incomplete 3. SCA

0 days Incomplete 4. AO

Select Action:
Initiate Workflow

Package Name:


Comments:

Initiate Workflow **Back**

© 2024 74

74

BAI eMASS Security Authorization Decision

CONTROLLED UNCLASSIFIED INFORMATION					
Security Authorization Decision					
System / Project Name eMASS RMF System	CCS/AFA OSD	System ID 1	System Type IS Major Application	Impact High	
DITPR ID 00000		DoD IT Registration Number			
Signature 	Authorization Decision Authorization to Operate w/Conditions (ATO w/Conditions)	Authorization Date: 13 Apr 2022	Type Authorization No	Other Information N/A	
		Auth. Termination Date: 13 Apr 2023			
		Connectivity Auth. Date: N/A			
		Connectivity ATD: N/A			
(1) Terms / Conditions for Authorization: Sample Terms / Conditions for Authorization					
Connectivity	CCSD Number	Circuit Owner	CCSD Location	CCSD Support	
ATDNet	-	No	-	-	

© 2024

75

75

BAI Plan of Action and Milestones (POAM)

Results from:

- Initial risk assessment
- Internal Security Testing
- Security Assessment Report
- May not be required when deficiencies are remediated during assessment or prior to authorization package submission – depends on the organization

Remediation:

- Identifies residual vulnerabilities, weaknesses, deficiencies
- Defines resources (personnel, funding, etc.) to accomplish tasks
- Establishes schedule and milestones in meeting the tasks
- Recommendation to complete before or after implementation

POAM is a living document

© 2024

76

76

BAI External Providers & Common Controls

- For security controls given by external provider, e.g.
 - contracts
 - interagency agreements
 - lines of business arrangements
 - licensing agreements, and/or
 - supply chain arrangements
 - etc.
- Provider must generate information needed for AOs to make risk-based decisions
- Authorization package includes documentation referencing such controls
- For external providers, ATO means controls are approved for inheritance

© 2024

77

77

BAI Authorize Summary Tasks and Responsibilities

Step 5: AUTHORIZE THE SYSTEM		
RMF Tasks	Per DoD KS Primary Responsibility	Per DoD KS Stakeholders
Prepare the POAM	ISO PM/SM	AO or AODR Common Control Provider (Owner) Information Owner/Mission Owner ISSM SISO
Submit Security Authorization Package	AO or AODR	Risk Executive (Function) SISO
AO conducts final Risk Determination	Authorizing Official or Designated Representative	Risk Executive (Function) SISO
AO makes authorization decision	AO	AODR CIO ISO or PM/SM Risk Executive (Function) SISO

© 2024

78

78

BAI Course Activity

- Refer to Course Guide to update "Authorize Concepts Review Quiz"



© 2024

79

79

BAI

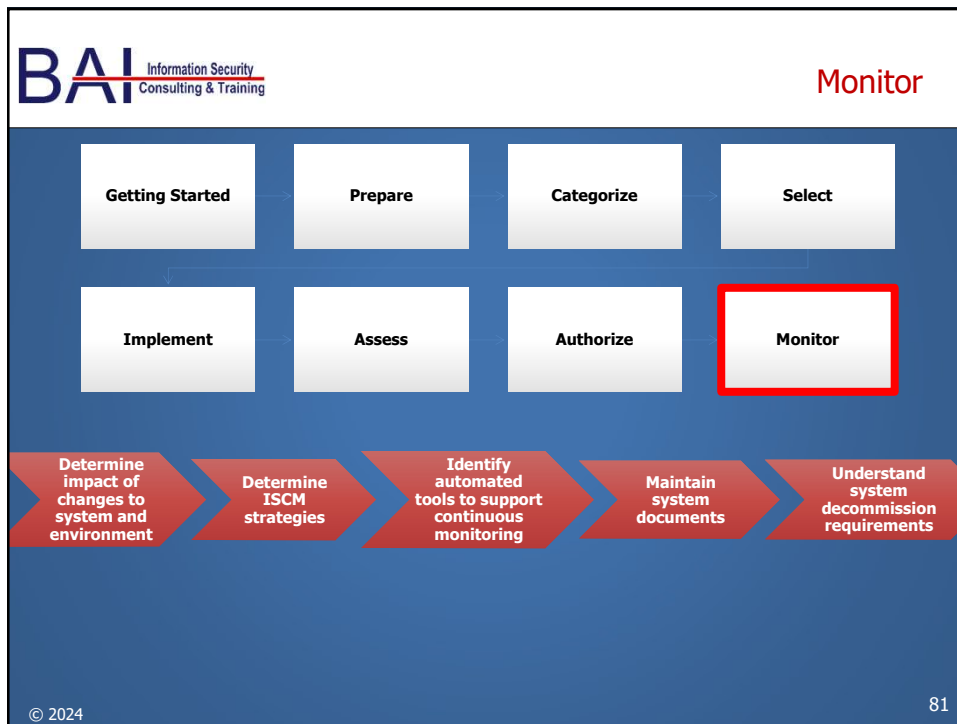
1. What are the key documents that are part of the Authorization Package?
2. What support documentation or information must an external provider of controls generate for AOs to make risk-based decisions?



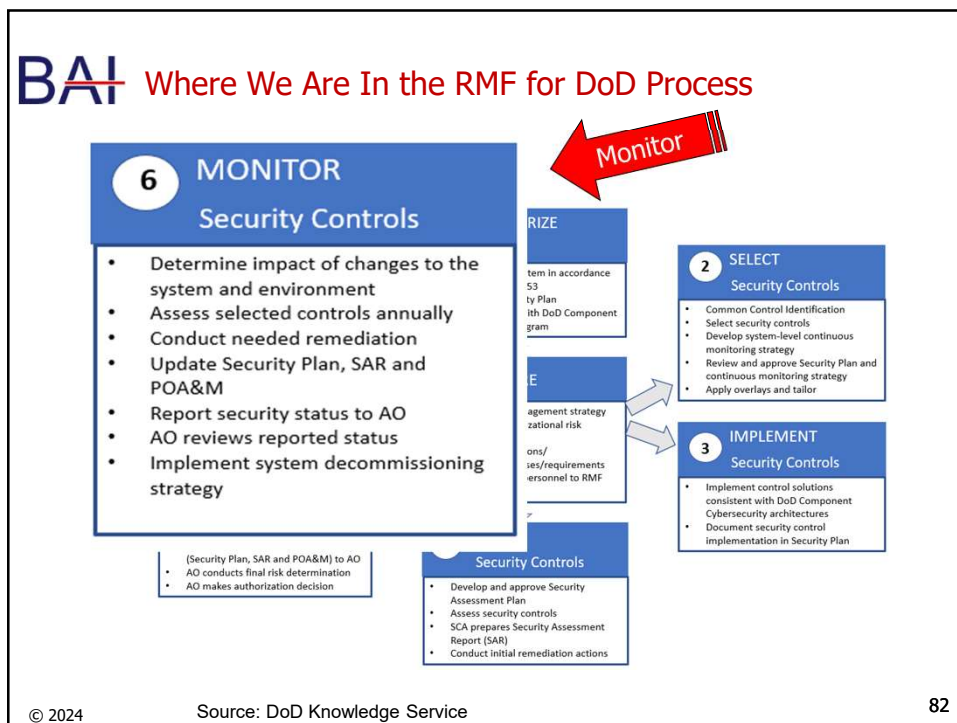
© 2024

80

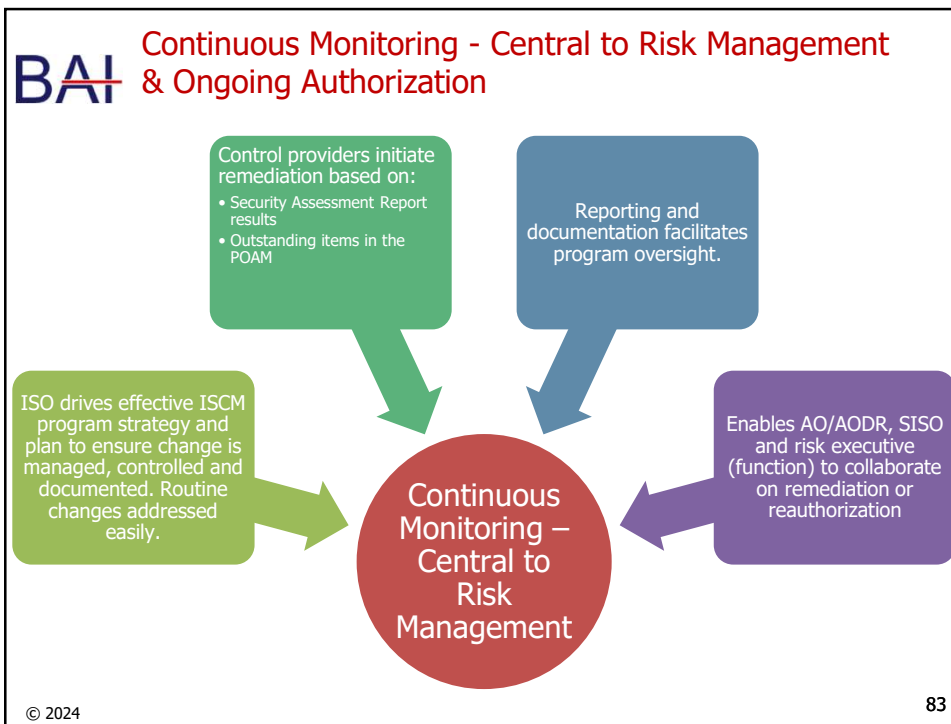
80



81



82



83

BAI ISCM Resources

- Knowledge Service
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST Special Publication 800-137

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

Information Security Continuous
Monitoring (ISCM) for Federal Information
Systems and Organizations

Kelley Dempsey
Nirali Shah Chawla
Arnold Johnson
Ronald Johnston
Alicia Clay Jones
Angella Orlough
Matthew Scholl
Kevin Stone

INFORMATION SECURITY

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

SEPTEMBER 2011

© 2024 84

84

BAI ISCM Program

- On demand access to security-related information:
 - Enables timely risk management decisions
 - Includes authorization decisions
- Requires frequent updates to RMF documentation (SSP, SAR, POAM, milestones), HW/SW inventories, other relevant system information
- Leverages automation
- Output is best when it is:
 - Specific, measurable, actionable, relevant, timely
- Goal is to maintain ATO - reauthorization may be time- or event-driven

© 2024

85

85

BAI ISCM Implementation - Process Overview

- Define the ISCM strategy
- Establish an ISCM program
- Implement the ISCM program
- Analyze and Report findings
- Respond to findings
- Review & Update ISCM strategy and program.



Figure 3-1. ISCM Process

© 2024

86

86

NIST Special Publication 800-137A

**Assessing Information Security
Continuous Monitoring (ISCM)
Programs:**

Developing an ISCM Program Assessment

Published May 2020, this NIST publication discusses the future assessment of the Information Security Continuous Monitoring (ISCM) program for federal organizations.

© 2024

87

87

- Organization is evaluated to determine whether the ISCM is effectively managing the organization's security posture commensurate with risk.
- ISCM program assessment is based on evaluation criteria derived from multiple sources.
 - Development of ISCM assessment criteria through Program Assessment Elements and Element Attributes described in an Element Catalog
 - Assessment through judgement values and scoring
 - Elements relate to one of the six steps involved in the ISCM process, as described in NIST SP 800-137
- Assessment evaluates the program itself, not the results of the continuous monitoring activities or the technologies used.
- Goal is to provide organizations with recommendations to improve the ISCM program and thereby manage and reduce organizational risk.

© 2024

88

88

BAI FISMA and OMB Requirements

- 3 years: systems to be reassessed/reauthorized
 - Still early days for support of ongoing authorization
 - ISCM - enabler for continuous reauthorization
- Provides leadership essential information, including:
 - ISCM activities
 - new vulnerabilities
 - mitigation plan for vulnerabilities
- Organization Program Management controls help ensure AO access to current status.

© 2024

89

89

BAI ATO 3-yr Maintenance

- ISO verifies required changes with security impact analysis
- Assess impact for baseline changes per:
 - new vulnerabilities/ emerging threats
 - HW/SW and firmware upgrades
 - hosting networks or facilities
 - managing configuration
 - independent evaluations (e.g., penetration tests)
 - external agency input (e.g., OIG, Government Accountability Office (GAO))



© 2024

90

90

BAI Status Reporting

- Provides leadership essential information, including:
 - ISCM activities
 - new vulnerabilities
 - mitigation plan for vulnerabilities
- Organization Program Management controls help ensure AO access to current status.
- Organization defines system level format/timing, e.g.:
 - Event-driven: System compromises or breaches
 - Time-driven: Weekly, monthly, quarterly
 - Typically, both: event- and time-driven
 - Updates to risk management information may be based on federal and organizational policies

© 2024

91

91

BAI Monitoring Frequencies

- Monitoring frequencies vary according to type of control, priorities and feasibility
- Timing, e.g., annually, quarterly, monthly, daily
- May be adjusted:
 - To response to security incidents
 - Based on problems with control implementation
 - Changes to systems and system components that have a significant impact
 - According to organizational information systems
 - Based on environments of operation
 - According to emerging threats and vulnerabilities

© 2024

92

92

BAI System Removal & Decommissioning

- Assess impact to inherited relationships
- Update tracking (e.g. inventory systems)
- Apply relevant controls, e.g.:
 - Dispose of artifacts and documentation per classification
 - Media sanitization
 - Configuration management and control
- Review Information Enterprise for impact, e.g.:
 - key management
 - identity management
 - vulnerability management
- Notify stakeholders
- Update SP with system's decommissioned status

© 2024

93

93

BAI Maintaining Documentation

- Provide visibility into security posture, e.g.
 - Security Plan
 - Describes/recommends control changes/improvements
 - New vulnerabilities/associated risk
 - Security Assessment Report (SAR):
 - Effectiveness of modified or added controls
 - POAM:
 - Reports plan to address new vulnerabilities
- Do not modify or destroy original information
- Needed for oversight, management and auditing
- Maintain strict configuration management control



© 2024

94

94



Assessment, Authorization, Monitoring Results/Artifacts

- Evidence-based Security Control artifacts
- POA&M Summary List
- Continuous Monitoring Plan/Strategy
- Policy for Information System Continuous Monitoring Program
- Completed eMASS Record



© 2024

95

95



Monitor Summary Tasks and Responsibilities

Step 6: Monitor			
RMF Tasks	Per DoD KS Primary Responsibility	Per DoD KS Stakeholders	
Determine impact of changes to the system and environment	ISO ISSM	SCA AO/AOR Common Control Provider	IO SISO Risk Executive (Function)
Assess selected controls annually	ISSM	AO or AODR CIO Common Control Provider IO	ISO SISO System Security Engr.
Conduct needed remediation	ISO PM/SM	AO or AODR IO Common Control Provider	ISSE ISSM SCA
Update security plan, SAR and POAM	ISO PM/SM	AO Common Control Provider	IO ISSM SCA
Report security status	ISSM	AO Common Control Provider	ISO PM/SM SCA
AO reviews reported status	AO or AODR	ISSM PM/SM Risk Executive (Function)	SCA SISO
Implement decommissioning strategy	ISO PM/SM	AO or AODR IO ISSM	SISO System Security Engr.

© 2024

96

96

BAI Monitor Process Review

- What are some of the tasks that take place during this final step of RMF?
- What are some of the ways an ISCM program can support the notion of ongoing authorization?



© 2024

97

97

BAI Optional Activity

- Refer to Activity Course Guide
"Maintaining Current Documentation
During the Monitoring Phase"



© 2024

98

98

BAI Thank you for attending!

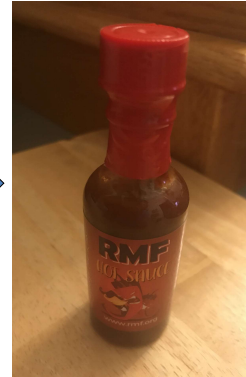
BAI Information Security
Consulting & Training

RMF Resource Center

1-800-RMF-1903

<https://rmf.org>

E-mail: rmf@rmf.org



Always evolving to meet your needs!

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

© 2024

99