Panel: Special Publication 800-53A Security Control Assessment Procedures and Assessment Cases

4th Annual Security Automation Conference

September 24, 2008

Background

- SP 800-53A assessment procedures for security controls defined in SP 800-53.
- Assessment cases.
- Panel structure and format.

Panel Members

- Arnold Johnson, NIST – Panel Moderator
- Gary Stoneburner, The Johns Hopkins University/Applied Physics Laboratory (JHU/APL)

  Special Publication 800-53A

  Guide for Assessing the Security Controls in Federal Information Systems

  Building Effective Security Assessment Plans

- Bennett Hodge, Booz Allen Hamilton

  Assessment Cases

  For Special Publication 800-53A

- Adam Oline, Department of Justice

  CSAM C&A Web

  SP 800-53A and Assessment Cases: Implementation and Automation

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Special Publication 800-53A

Guide for Assessing the Security Controls in Federal Information Systems

Building Effective Security Assessment Plans

4th Annual Security Automation Conference

September 24, 2008

Gary Stoneburner

The Johns Hopkins University/Applied Physics Laboratory (JHU/APL)

Control Assessment: Answer the Mail / Cost-Effective

- Answer the mail: Get the information necessary to make an informed decision
  - Primary: Information gathering; what has been achieved
  - Secondary: Quality improvement (cannot test in quality)
- Cost-effective: When the needed info is obtained – stop!
  - What is already known is not rendered invalid just because this assessor did not obtain it
  - Weak claim only warrants limited assessment
  - Strong claim must be supported by basic reasons to believe that claim – if not, further assessment is probably not useful

SP 800-53A Purpose

- Guidelines for building effective security assessment plans and
- A comprehensive set of procedures for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government.

What is SP 800-53A?

- Not a replacement for SP 800-53
  - SP 800-53A is companion guidance, SP 800-53 remains the definitive control catalog and control selection process
- Not a set of required assessment actions
  - SP 800-53A guidance describes a flexible assessment process, giving what needs to be determined, not a mandated how
  - SP 800-53A has been developed with the intention of enabling organizations to tailor and supplement the basic assessment procedures provided.
- SP 800-53A provides a common process for organizations to use in developing the assessment plan that cost-effectively 'answers the mail' for a given assessment.

SP 800-53 Defines Types of Actions aka Assessment "Methods"

- Examine
  - Review, study, analyze documentation
  - Observe, inspect mechanisms or activities
- Interview
  - Conduct discussions with individuals
- Test
  - Exercise activities or mechanisms

SP 800-53A Defines Levels of Rigor

- Depth (how 'precise')
  - Generalized – high level (read, general discussion, basic tests)
  - Focused – more in-depth (study, in-depth discussion, added tests)
  - Detailed – Extensive (analyze, probing discussion, thorough testing)
- Coverage (how 'broad')
  - Representative – Enough to indicate overall (perhaps random sample)
  - Specific – Includes specific entities not just random sample
  - Comprehensive – Enough to verify overall

ASSESSMENT PROCEDURE

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Restatement of SP 800-53
For convenience– Not as replacement

Supplemental Guid pt of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

AC-6.1 ASSESSMENT OBJECTIVE:

Determine if:

(i) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks; and

(ii) the information system enforces the most restrictive set of rights/privileges or accesses needed by users.

POTENTIAL ASSESSMENT METHODS AND OBJECTS:

Examine: [SELECT FROM: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. (M) (H)

Interview: [SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. (H)

Using SP 800-53A

- Get Assessment Procedure for each control to be assessed
  - Which controls? Well that depends …
    - Complete assessment or part of on-going monitoring
    - Only controls in security plan are assessed (How they got there is not germane – security plan states what is intended.)
- Decide on methods and objects needed
  - SP 800-53A gives likely 'pick list' – not mandatory set
  - Take into account existing information and other specifics of this assessment
- Order procedures to take advantage of information gained in one procedure that supports others – assessment efficiency

Flexibility has Ramifications

- SP 800-53A provides flexibility so organizations you can achieve assessments that are cost-effective and provide the information you needed (not demanding the effort someone else thinks you should expend to get data you might not need)
- Yet with flexibility comes the need to build the assessment plans and the resources needed to do so
- But not all organizations have the resources needed, making flexibility, while necessary in the NIST guidance, a problem as well.
    - The solution – assessment cases …

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Assessment Cases

For Special Publication 800-53A

4th Annual Security Automation Conference

September 24, 2008

Bennett Hodge

CISSP, CISA, CISM

Booz Allen Hamilton

Purpose of Assessment Cases

- Provide comprehensive implementation guidance for NIST SP 800-53A assessment procedures.
- Establish a *likely* set of *recommended* assessor actions that can be tailored and supplemented to evaluate federal information system controls.
- Promote cost-effectiveness and efficiencies in development and execution of control assessment plans.

Assessment Cases Background

- The concept of assessment cases emerged during ongoing development of SP 800-53A assessment procedures.
- Some organizations preferred the *flexibility* of the high-level assessment procedures found in Appendix F of SP 800-53A.
- Some organizations preferred a more prescriptive approach for employing these high-level assessment procedures.
- Assessment Case Development Project initiated to "bridge the gap"; using *prescriptive* set of assessor actions to implement *flexible* framework of *high-level* assessment procedures.

Assessment Case Development Project

- Initiated as inter-agency taskforce with Departments of Justice, Energy, Transportation, and Intelligence Community; mission objectives being:
  - Engage experienced assessors (supporting federal agencies) to develop assessor actions for employing SP 800-53A assessment procedures.
  - Provide organizations and assessors supporting those organizations with a *recommended checklist* of specific assessor actions most likely to be employed for each assessment procedure.
  - Encourage ongoing community input to facilitate continuous improvement and cost-effectiveness of assessment cases.

Key Assessment Case Elements

- "*Potential Assessment Sequencing*" identifies controls most likely *related* to the specific control being assessed; facilitates cost-effective and efficient development of assessment plans.
  - Precursor Controls: Assessed *prior to* specific control being assessed.
  - Concurrent Controls: Assessed *parallel to* specific control being assessed.
  - Successor Controls: Assessed *after* specific control being assessed.
- "*Potential Assessor Evidence Gathering Actions*" provides recommended assessment methods (*examine, interview, test*), assessment objects, coverage, and depth to determine control effectiveness.
- "*Notes to the Assessor*" provides helpful information for assessors to better understand intent of the control or how to assess the control more effectively and efficiently.

ASSESSMENT CASE

CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

ASSESSMENT – Base Control, Part 1 of 1

Assessment Information from SP 800-53A

CP-10.1
CP-10.1.1

ASSESSMENT OBJECTIVE:

Determine if the organization provides and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.

POTENTIAL ASSESSMENT METHODS AND OBJECTS:

Examine: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records]. **(L) (M) (H)**

Test: [*SELECT FROM:* Automated mechanisms implementing information system recovery and reconstitution operations]. **(M) (H)**

Additional Assessment Case Information

POTENTIAL ASSESSMENT SEQUENCING:

PRECURSOR CONTROLS: CP-4

CONCURRENT CONTROLS: NONE

SUCCESSOR CONTROLS: NONE

Action Step	Applicability	Potential Assessor Evidence Gathering Actions
CP-10.1.1.1	L M H	**Examine** the security plan, information system design documents, or other relevant documents; reviewing for the measures to be employed for recovery and reconstitution of the information system to a known secure state after disruption or failure.
CP-10.1.1.2	M H	**Test** an agreed-upon representative sample of the measures identified in CP-10.1.1.1; performing focused testing to determine if the information system is recovered and reconstituted to a known secure state.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

CSAM C&A Web

SP 800-53A and Assessment Cases: Implementation and Automation

4th Annual Security Automation Conference

September 24, 2008

Adam Oline

Department of Justice

ISSLOB Shared Service Center for FISMA Reporting

Shared Service Center Background

- Cyber Security Assessment and Management (CSAM) C&A Web originated as Department of Justice in-house application supporting C&A process, POA&M management, and FISMA Reporting
- DOJ designated as a Shared Service Center for FISMA Reporting by OMB through ISSLOB initiative in 2007
- As of today, 12 Federal Agencies have selected the DOJ Shared Service Center as their FISMA Reporting solution, 7 have implemented CSAM, remaining 5 to come online soon utilizing DOJ hosting service

CSAM Prior Assessment Approach

Control AC-2: The organization manages information system accounts…

Test Step AC-2.1: Interview System Owner to determine if…

Expected Result AC-2.1.1: Accounts are managed…

Expected Result AC-2.1.2: Temporary accounts are disabled after…

Test Step AC-2.2 Examine document…

Expected Result AC-2.2.1: Authorizations include…

- "One test step fits all"
- Original implementation of SP 800-53 control assessments in CSAM followed model in early drafts of SP 800-53A
- Prescriptive test steps
- Expected results derived from test steps
- This approach has been used at DOJ from FY06 to FY08

CSAM New Assessment Approach

Control AC-2: The organization manages information system accounts

Assessment Objective AC-2.1: Determine if: (i)…, (ii)…, & (iii)…

Expected Result AC-2.1.1: (i) Accounts are managed…

Action Step AC-2.1.1.1: Interview the System Owner to determine if…

Action Step AC-2.1.1.2: Examine authorizations to determine if…

Action Step AC-2.1.1.3: Test the system to determine if…

Action Step AC-2.1.1.U1: *User defined step*

- "Some test steps fit better than others"
- Following current SP 800-53A guidance, CSAM to utilize new approach in FY09
  - Focus on **what** to determine
  - Flexibility in **how** to determine
- Assessor selects from **potential** action steps to provide appropriate level of confidence in assessment of security control effectiveness
- CSAM is flexible
  - Potential actions pre-populated based on current assessment case project content
  - Agency implementing CSAM may author additional action steps
  - Assessor selects appropriate action steps and/or generates user-defined action steps

CSAM Automation

Security Life Cycle		CSAM Automation Support
CATEGORIZE Information System	Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.	**Wizard facilitates selection of SP 800-60 Information Types and impact levels, computes high watermark Security Category.**
SELECT Security Controls	Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.	**Baseline controls automatically selected based on category and other factors, user may tailor and supplement further.**
IMPLEMENT Security Controls	Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.	**CSAM directly supports many management controls (CA, PL, RA). Common control status available online.**
ASSESS Security Controls	Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).	**Controls, objectives, and potential actions are pre-loaded; recommendations pre-selected based on category; user tailors as needed.**
AUTHORIZE Information System	Determine risk to organizational operations and ass individuals, other organizations, and the Nation; if acceptable, authorize operation.	**Reduction of paperwork-drill: user enters data, application generates standardized SSP (including RA), SAR, POA&M.**
MONITOR Security Controls	Continuously track changes to the information system that may affect security controls and reassess control effectiveness.	**Prior results maintained online, CSAM supports Agency, Component, and System-level scheduling of monitoring tasks.**

For Further Information

- Program Manager: Mark Philip, DOJ
  - Mark.E.Philip@usdoj.gov
  - 202-353-3794

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Questions?

Assessment procedures and assessment cases:
http://csrc.nist.gov/groups/SMA/fisma/assessment.html