NIST Cybersecurity Risk Management Conference

Share and explore best practices, receive and discuss stakeholder input on key cybersecurity and privacy risk management topics, such as the Risk Management Framework, Supply Chain Risk Management, and Privacy Engineering.

November 7-9, 2018

Renaissance Baltimore Harborplace Hotel

202 E Pratt St, Baltimore, MD 21202

For more information and to register: https://go.usa.gov/xPR9Q

NIST SP 800-171A

Assessing Security Requirements for Controlled Unclassified Information

Controlled Unclassified Information (CUI)
Security Requirements Workshop
18 October 2018

NIST/ITL/CSD Public Comment Process

Be Part of the Solution

- All publications produced by CSD go through the public comment process
- Your voice will be heard!!
- Receive notifications of newly posted drafts (and more) by subscribing at http://csrc.nist.gov/publications/subscribe.html
- There may be one or more drafts of a given publication
- Drafts are published at http://csrc.nist.gov/publications/PubsDrafts.html
- Lengths of public comment periods vary

SP 800-171A

Assessing Security Requirements for CUI

- Final publication 13 June 2018
- Provides a methodology and procedures (potential assessment methods and objects) to determine if security safeguards are implemented correctly, operating as intended, and satisfy CUI requirements
  - Self-Assessment
  - Independent/third party Assessment
  - Sponsoring organizations (e.g., government agencies)

SP 800-171A and SP 800-53A Alignment

SP 800-171A is aligned with SP 800-53A as follows:

- An assessment *procedure* for each security requirement in SP 800-171 is provided
- Each assessment procedure includes:
  - An assessment *objective* in the form of a determination statement
  - **Potential** assessment *objects* relevant to each requirement
  - Three **potential** assessment *methods* to apply to objects
- **No expectation** that all assessment methods or objects are selected for each assessment procedure
  - The number of objects and types of methods selected support varying degrees of rigor based on customer-defined depth and coverage attributes

Assessment Objectives

- A set of ***determination statements*** related to the particular control under assessment
- Each determination statement is closely linked to the content of the security requirement
- The linkage ensures traceability of assessment results to security requirements

Assessment Objects

- Four types of objects:
  - **Specifications**: Document-based artifacts (e.g., policies, procedures, plans, specifications, drawings)
  - **Mechanisms**: Hardware, software, and firmware safeguards (e.g., I&A mechanisms, access control devices, cryptographic mechanisms)
  - **Activities**: Protection-related actions that involve people (e.g., monitoring network traffic, conducting system backups, incident handling)
  - **Individuals**: People applying the specifications, mechanisms, or activities
- Are **not** exhaustive lists

Assessment Methods

- **Examine**: Reviewing, inspecting, observing, studying, or analyzing one or more assessment objects to obtain evidence of control effectiveness
- **Interview**: Conducting discussions with organizational staff to obtain evidence of control effectiveness
- **Test**: Exercising one or more assessment objects under specified conditions to compare actual with expected behavior

SP 800-171A Assessment Procedure

3.1.4	**SECURITY REQUIREMENT** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.4[a]	*the duties of individuals requiring separation are identified.*
	3.1.4[b]	*responsibility for duties that require separation are assigned to separate individuals.*
	3.1.4[c]	*access privileges that enable individuals to exercise the duties that require separationare granted to separate individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing divisions of responsibility and separation of duties; security plan; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Mechanisms implementing separation of duties policy].	

Depth, Coverage, and Assurance

- Depth - Addresses level of detail of assessment
- Coverage - Addresses scope/breadth of assessment
- Attributes for Depth and Coverage:
  - Basic
  - Focused
  - Comprehensive
- As the attributes increase, the rigor of the assessment and thus the *confidence* that requirements are implemented correctly and operating as intended increase (i.e., greater ***assurance*** is provided)

Determining Appropriate Depth/Coverage: Examine

- **Depth** Attributes
  - **Basic** – high level reviews/inspections; limited evidence
  - **Focused** – more in-depth reviews; substantial evidence
  - **Comprehensive** – thorough reviews; extensive evidence
- **Coverage** Attributes – types and number of objects
  - **Basic** – examine a representative sample of objects
  - **Focused** – examine representative sample plus additional objects of particular importance to achieving objectives
  - **Comprehensive** – examine a sufficiently large sample of objects and additional objects of importance

Determining Appropriate Depth/Coverage: Interview

- **Depth** Attributes
  - **Basic** – broad-based, high level discussions; generalized
  - **Focused** – more in-depth discussion; more specific
  - **Comprehensive** – probing discussion; very specific
- **Coverage** Attributes – type/number of interviewees
  - **Basic** – interview a representative sample of staff in key roles
  - **Focused** – interview representative sample plus additional specific staff of particular importance to achieving objectives
  - **Comprehensive** – interview a sufficiently large sample of staff plus additional specific staff of importance

Determining Appropriate Depth/Coverage: Test

- **Depth** Attributes – types of testing to be conducted
  - **Basic** – black box testing; no knowledge of internal structure
  - **Focused** – gray box testing; some knowledge of structure and limited architectural information
  - **Comprehensive** – white box testing; explicit knowledge of structure and extensive architectural information
- **Coverage** Attributes – type/number of objects to test
  - **Basic** – test a representative sample of objects
  - **Focused** – test representative sample plus additional objects of particular importance to achieving objectives
  - **Comprehensive** – test a sufficiently large sample of objects plus additional specific objects of importance

App D – Assessment Methods

Method	**EXAMINE** The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.		
Objects	***Specifications***	Examples: policies, plans, procedures, system requirements, designs.	
	Mechanisms	Examples: functionality implemented in hardware, software, firmware.	
	Activities	Examples: system operations, administration, management, exercises.	
Attributes	***Depth***	Addresses the rigor of and level of detail in the *examination* process.	
		Basic	Examination that consists of high-level reviews, checks, observations, or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation. Examples include: functional-level descriptions for mechanisms; high-level process descriptions for activities; and documents for specifications. Basic examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.
		Focused	Examination that consists of high-level reviews, checks, observations, or inspections **and more in-depth studies and analyses** of the assessment object. This type of examination is conducted using a **substantial** body of evidence or documentation. Examples include: functional-level descriptions **and where appropriate and available, high-level design information** for mechanisms; high-level process descriptions **and implementation procedures** for activities; and documents **and related documents** for specifications. **Focused** examinations provide a level of understanding…
		Comprehensive	Examination that consists of high-level reviews, checks, observations, or inspections and more in-depth, **detailed, and thorough** studies and analyses of the assessment object. This type of examination is conducted using an **extensive** body of evidence or documentation. Examples include: functional-level descriptions and where appropriate and available, high-level design information, **low-level design information, and implementation information** for mechanisms; high-level process descriptions and **detailed** implementation procedures for activities; and documents and related documents for specifications. **Comprehensive** examinations provide a level of understanding of the security…

Assessment Plan

- Assessors develop an assessment plan that specifies the assessment method(s) and object(s) needed to meet each assessment objective
- The specified methods and objects are sufficient to ensure that the evidence needed to support the degree of rigor can be obtained
- Assessors conduct the assessment in accordance with the assessment plan

Assessment Findings

- Findings are based on the evidence collected from applying the assessment methods to objects
- Assessment activities produce findings:
  - Satisfied
  - Other than Satisfied
- For other than satisfied results, assessors specify rationale and note any partial "credit"
- Additional information can be included (criticality of weakness, potential adverse effects, etc.) at organizational discretion

Security Requirement Discussion*

3.1.4	**SECURITY REQUIREMENT** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
	DISCUSSION Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

*Originally published in 171A drafts but moved to 171R1 errata dated 7 June 18 as Appendix F

SP 800-171/171A Additional Resources

- Supplemental materials:
  - https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
  - SSP Template (doc)
  - POAM Template (doc)
  - Mapping of 171 security requirements to Cybersecurity Framework (xls)
- NIST's Manufacturing Extension Partnership's **Handbook 162**, NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements
- CUI registry (managed by National Archives and Records Administration - NARA) https://www.archives.gov/cui

NIST Contact Information

Project Leader and NIST Fellow

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Senior Information Security Specialist and Team Lead

Victoria Yan Pillitteri
(301) 975-8524
victoria.yan@nist.gov

Senior Information Security Specialist

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Comments: sec-cert@nist.gov (goes to all of the above)

Web: https://csrc.nist.gov/Projects/Risk-Management