Ongoing Authorization

Federal Computer Security Management Forum

September 10, 2018

Kelley Dempsey

Computer Security Division
Information Technology Laboratory

Ongoing Authorization in SP 800-37 R2

- Monitor Step, Task M-6
- The NIST OA guidance from the June 2014 white paper is incorporated into SP 800-37 R2
- There are **no** substantive changes to the OA guidance in SP 800-37 R2
- Expanded Authorization guidance, including OA, is provided in SP 800-37 R2, Appendix F
- May be applied to:
  - Authorizations to Operate
  - Common Control authorizations
  - Type and Facility authorizations

Ongoing Authorization

- The risk determinations and risk acceptance decisions taken at agreed upon and documented frequencies subsequent to the initial authorization (during ops phase)
- Is time-driven and may also be event-driven
- Dependent on a robust ISCM program to provide near real-time system security-related information
- Considers/includes not only technology but also people, processes, etc.

Conditions for OA Implementation

1. AO has granted an initial ATO IAW the RMF, and the system or common control has entered the operational phase
2. A robust ISCM program is in place that monitors all implemented controls:
   - at the appropriate frequencies
   - with the appropriate degree of rigor
   - IAW the organization's ISCM strategy and NIST guidance

OA Frequency

- A discrete frequency (i.e., time-driven trigger) for OA is defined in accordance with:
  - SP 800-53 CA-6, Part C – update the security authorization at an organization-defined frequency
  - The organization's ISCM strategy
- Event-driven triggers for OA may also be defined by the org
  - Increase in defects from ISCM
  - Change in RA findings
  - New threat/vulnerability information
  - Significant changes (changes that affect security posture)
  - Etc.

RMF Tasks Under OA (1 of 2)

- Assess Step, Task A-6: Prepare POA&M
  - Process unchanged other than defect information being identified from output of ISCM in near-real time
- Authorize Step, Task R-1: Assemble & Submit Authorization Package
  - AO requires similar information found in the SAR, SSP, and POA&M
  - AO ideally retrieves the information via a security management & reporting tool
- Authorize Step, Task R-2: Risk Analysis and Determination
  - Process unchanged other than use of the security management & reporting tool or other automated tools for access to the necessary information

RMF Tasks Under OA (2 of 2)

- Authorize Step, Task R-4 – Authorization Decision
  - AO still responsible and accountable for understanding and accepting risk
  - Termination date for ATO does not have to be specifically stated as long as the ISCM program continues to provide the necessary security-related information; the discrete authorization frequency is specified instead.
- Monitor Step, Task M-6 – Ongoing Authorization
  - Replaces 37R1 Task 6-6, Ongoing Risk Determination and Acceptance
  - Is essentially the same task based on the same input from monitoring reports and same responsibility for the AO

RMF Monitor Step and Ongoing Authorization

- Organizational ISCM Programs must be mature before attempting ongoing authorization
- Leverage the security-related information gathered during monitoring to support ongoing authorization
  - As opposed to a static, point-in-time assessment
  - Security-related information from monitoring provides current information needed by Authorization Officials to maintain situational awareness and make informed authorization (risk) decisions
  - Support of ongoing authorization decisions is a factor in continuous monitoring frequency decisions
  - Security-related information supporting ongoing authorization should be made available to Authorizing Officials as a SEIM-style report (ideally)
  - Security-related information from manual monitoring is used when automated monitoring is not possible

Ongoing Assessment and OA

- Monitor Step, Task M-2: Ongoing Assessment
- Assessing all implemented controls (including common controls) on an ongoing basis as part of the ISCM program
- Basically the “implement” step of ISCM

Assessment Considerations for OA

- Security-related information may be collected via automated tools or manually
- Information on **all** implemented controls is collected at the *determined* frequency
- Automated tools may not provide complete information for risk determinations because:
  - All implemented controls/control items are not assessed by tools
  - Tools cannot be used to assess specific technologies or platforms
  - More assurance is needed than is provided by tools
- Manually generated information is provided to the AO based on organizational procedures

Assessor Independence for OA

- Assessor independence requirements for moderate and high impact systems **still apply** as described in:
  - SP 800-53 security controls CA-2(1) and CA-7(1)
  - SP 800-37 R2 Assess Step, Task A-1, Assessor Selection

Contact Information

Project Leader and NIST Fellow

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

Administrative Support

Jeff Brewer
(301) 975-2489
jeffrey.brewer@nist.gov

Senior Information Security Specialist

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

Team Lead and Senior Information Security Specialist

Victoria Pillitteri
(301) 975-8542
victoria.pillitteri@nist.gov

Information Security Specialists

Ned Goren
(301) 975-5233
nedim.goren@nist.gov

Jody Jacobs
(301) 975-4728
jody.Jacobs@nist.gov

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

Web: csrc.nist.gov/sec-cert