Ongoing Authorization

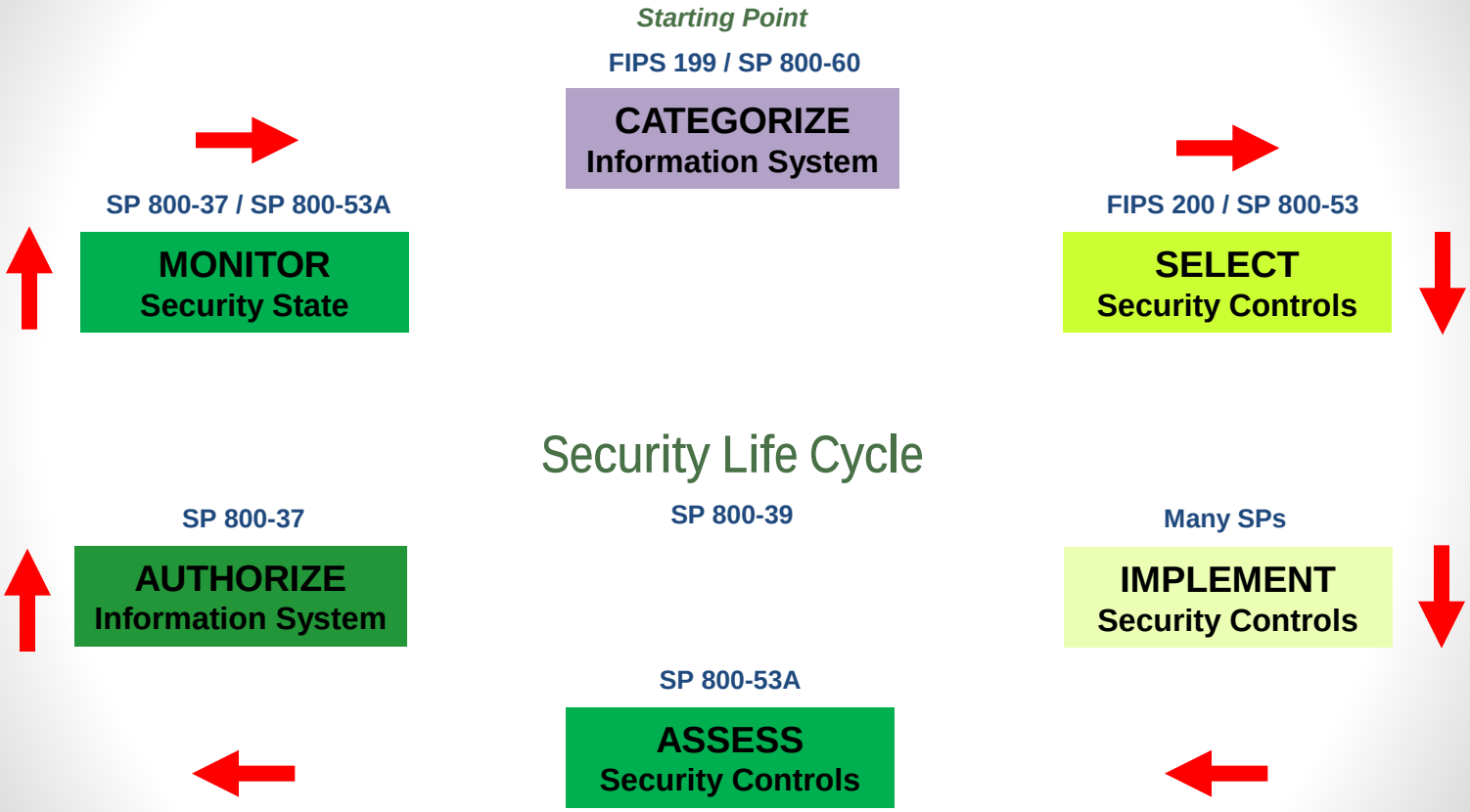
Clarifying and Amplifying Guidance

April 10, 2014

Kelley Dempsey

Computer Security Division
Information Technology Laboratory

Risk Management Framework



OA Guidance

- OMB Memo M-14-03
- STILL IN DRAFT!!
- Focused on adapting existing guidance on security authorization to ongoing authorization
  - RMF Step 5 (Authorize step) tasks still apply
  - Dependent on ISCM/ongoing assessment

Three Types of Security Authorization

- Initial Authorization
  - Initial risk determination/acceptance conducted prior to operations/maintenance phase of SDLC
- Ongoing Authorization
  - Follow-on risk determinations/acceptances at agreed-upon frequencies or after defined events (time- or event-driven triggers)
- Reauthorization
  - Static risk determination/acceptance occurring during the operations/maintenance phase of SDLC as a result of an event-driven trigger

Conditions for OA Implementation

- The initial Authorization to Operate has been granted as the result of a complete, zero-base review of the system and the system is operational
- A robust ISCM program is in place capable of monitoring all implemented security controls with appropriate rigor and at appropriate frequencies in accordance with:
  - SP 800-53 security control CA-7, *Continuous Monitoring*
  - SP 800-53A
  - SP 800-137

ISCM Information Generation

- To support OA:
  - Information on all implemented controls is collected at the determined frequency
  - Information may be collected using automated tools or via manual collection
  - Manually collected information is entered into the security management and reporting tool

Independence Requirements

- Assessor independence requirements for moderate and high impact systems still apply as defined in:
  - SP 800-53 security control CA-7 (1)
  - SP 800-37 Task 4-1

OA Criteria

- Discrete frequency 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
- Time-Driven and Event-Driven Triggers for OA
  - Time-Driven trigger is the discrete frequency
  - Event-Driven triggers may also be defined by the organization
    - Increase in defects from ISCM
    - Change in RA findings
    - New threat/vulnerability information
    - Etc.

RMF Step 5 Tasks Under OA

- Task 5-1: Prepare POA&M
  - Process unchanged other than defect information being identified from output of ISCM in near-real time
- Task 5-2 – Assemble Security Authorization Package & Submit It
  - AO still requires the information from the SAR, SSP, and POA&M
  - AO retrieves the information via security management & reporting tool
- Task 5-3 – Determine Risk
  - Process unchanged other than use of the security management & reporting tool for access to the necessary information
- Task 5-4 – Determine if Risk is Acceptable
  - AO still responsible and accountable for understanding and acceptance for risk
  - Termination date for ATO does not have to be specifically stated as long as the org is following the ISCM strategy

Contact Information

NIST FISMA Project Leader

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

NIST *Administrative Support*

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

NIST Senior Information Security Researchers and Technical Support

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

Comments: sec-cert@nist.gov

Web: csrc.nist.gov/sec-cert