Ongoing Authorization

Transitioning to Near Real-Time Risk Management

August 19, 2014

Kelley Dempsey

NIST IT Laboratory

Computer Security Division

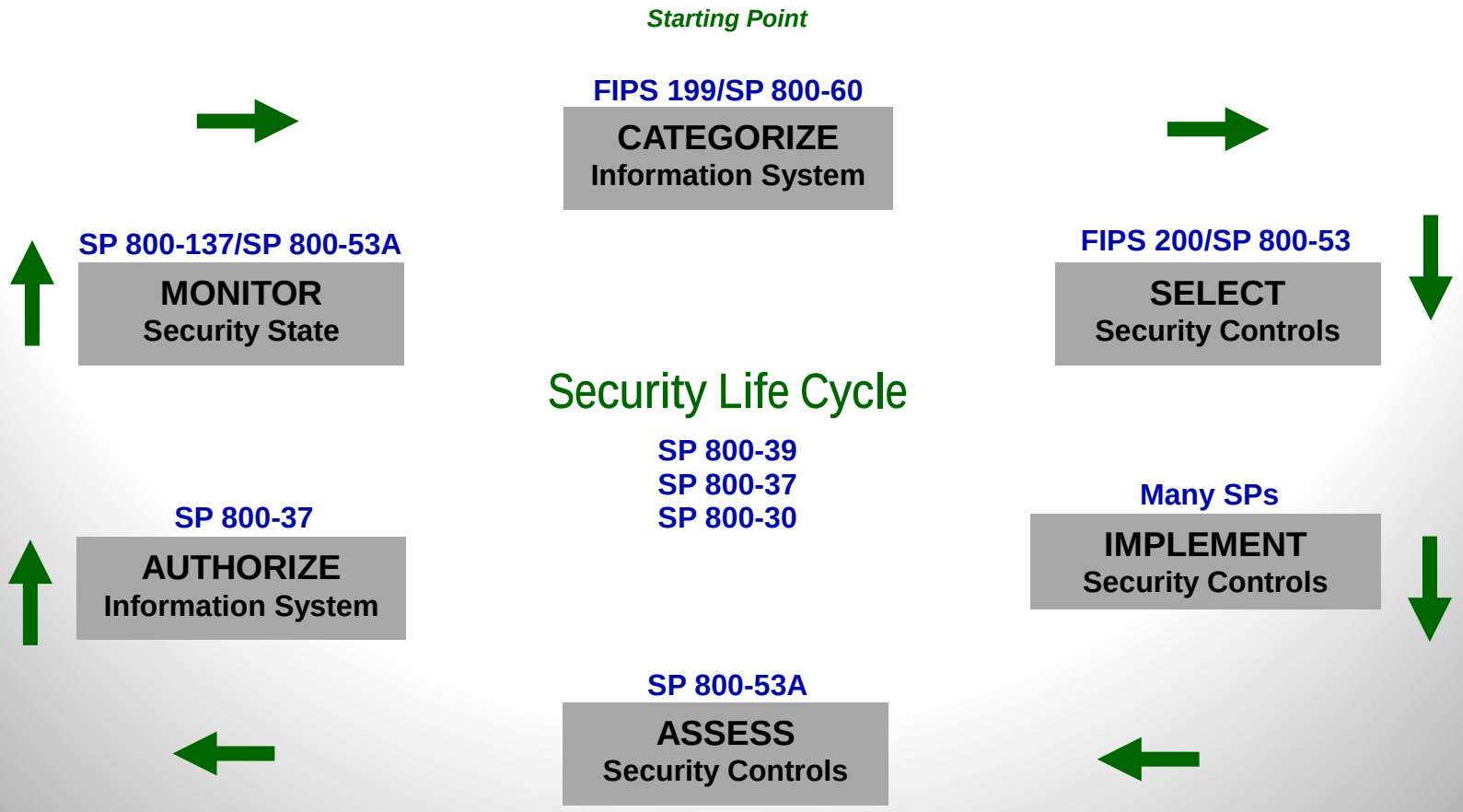
The Need for Supplemental Guidance

- Initial guidance on ongoing authorization (OA) is found in NIST SPs 800-37/800-137
- Terms related to OA are not well defined in those pubs, nor are *specific* conditions and criteria for moving to OA
- Will likely be incorporated into future versions of SPs 800-37 and 800-137

OMB Memo 14-03

The memo directs NIST to publish guidance establishing a process and criteria for federal agencies to conduct OA

Risk Management Framework



Where Does OA Fit within RMF Steps?

- Ongoing authorization is part of Step 5, Authorize
- Ongoing assessment is part of Step 6, Monitor
- Both ongoing authorization and ongoing assessment are **dependent** on the organization's Information Security Continuous Monitoring (ISCM) strategy and program

Security Authorization Definitions: Initial

- Initial Authorization - the initial (start-up) risk determination and risk acceptance decision based on a zero-base review, ideally conducted *prior to* operations phase
- Includes an assessment of all implemented security controls as documented in the system security plan

Security Authorization Definitions: Ongoing

- 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 a time- or event-driven authorization process
- Is dependent on the ISCM program to provide information about the system's near real-time security state

Security Authorization Definitions: Reauthorization

- Reauthorization - the static, single point-in-time risk determination/risk acceptance decision that occurs subsequent to the initial authorization
- May be a time- or event-driven authorization process conducted *during* operations phase
- Under OA, reauthorization is typically an event-driven action in response to an event that drives risk above organizational risk tolerance

Information Security Continuous Monitoring

- SP 800-137: Maintaining ongoing awareness of information security, vulnerabilities, and threats to support risk management decisions.
- Six steps:
  - Define ISCM strategy
  - Establish ISCM program (metrics, frequencies, tech arch)
  - Implement ISCM program
  - Analyze collected data and Report findings
  - Respond to findings
  - Review/Update ISCM program

Ongoing Assessment

- The continuous evaluation of the effectiveness of security control implementation
- Is *NOT* separate from ISCM
- Is a *subset of ISCM activities* (Steps 3 and 4)
  - Is initiated when the collecting of security-related information begins as part of ISCM Step 3, Implement (both automated and manual/procedural collection)
  - Continues as information is correlated, analyzed, and reported as part of ISCM Step 4, Analyze and Report

Conditions for OA Implementation

1. AO has granted an initial ATO IAW the RMF, and system has entered operational phase
2. 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

Process for OA Implementation

- The organization defines and implements a process to specifically designate that:
  - the system has satisfied the two conditions
  - the system has transitioned to ongoing authorization
- The AO formally:
  - acknowledges that the system is now being managed under the ongoing authorization process
  - accepts responsibility for performing necessary activities associated with the OA process
  - issues a new authorization decision document

Collecting Security-Related Info for OA

- To support OA, security-related info is generated for **all** implemented controls (including inherited common controls):
  - at the frequency specified in the ISCM strategy
  - using automated or manual/procedural methods
- Automated tools may not be sufficient because:
  - additional assurance is needed
  - tools don't cover all implemented controls/parts of controls
  - tools don't cover all technologies/platforms

Assessor Independence for OA

To support OA for moderate and high impact systems:

- security-related information (automated and manually/procedurally generated) is produced and/or analyzed by an entity that meets independence requirements defined in control CA-7(1)
- the independent entity is impartial and free from any perceived or actual conflicts of interest

OA Frequency

- Security control CA-6, Part c. requires updating the security authorization at an organization-defined frequency
- CA-6, Part c. reinforces the concept of OA
- Organizations define the frequency with which AOs review security-related information and determine if the risk continues to be acceptable
- Security-related information is typically delivered to the AO via a security management and reporting tool

Time-Driven Authorization

- Refers to the frequency of OA defined by the organization as part of CA-6, Part c.
- Time-driven OA frequency may (and probably should) be dependent on the system impact level
- AOs review security-related information with *at least* the organization-defined frequency

Event-Driven Authorization

- Necessitates an immediate review of security-related information by the AO
- Immediate review is *in addition to* the time-driven frequency defined in the ISCM strategy/CA-6c
- Organizations define event-driven *triggers* for ongoing authorizations and reauthorizations
- Trigger – indicators or prompts that cause an organization to react in some predefined manner

Event-Driven Triggers for OA

- New threat/vulnerability impact information
- Increased number of findings from ISCM program
- New mission/business requirements
- Change in AO
- Organizational thresholds being exceeded
- Significant changes:
  - in risk assessment findings
  - to the system, common controls, or environments of op

Event-Driven Triggers for Reauthorization

- When risk rises above the acceptable organizational risk tolerance due to, for example:
  - A catastrophic breach/incident
  - Failure of, or significant problems with, the ISCM program
- Reauthorization actions may necessitate a review of and changes to the ISCM strategy

RMF Step 5 (Authorize) Tasks - SO

- Task 5-1: Prepare the POA&M
  - Overall process is unchanged under OA
  - Specific weaknesses are identified using output of ISCM
- Task 5-2: Assemble and submit package to AO
  - Overall process is unchanged under OA
  - AO still requires the same information (SSP/SAR/POA&M)
  - SAR and POA&M info are generated from output of ISCM
  - *Ideally*, the information is delivered to the AO via automated reports

RMF Step 5 (Authorize) Tasks - AO

- Task 5-3: Determine the risk
  - Overall process is unchanged under OA
  - AO still reviews security-related info and determines risk IAW the organization risk management strategy
- Task 5-4: Determine if risk is acceptable
  - Overall process is unchanged under OA
  - AO is still responsible and accountable to explicitly understand and accept the risk
  - AO acknowledges risk continues to be acceptable or indicates risk is no longer acceptable

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

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

Administrative Support

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

Senior Information Security Researcher and Technical Support

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov