RMF 2.0 Prep Step Deep Dive

NIST SP 800-37 Revision 2

(Initial Public Draft)

May 2018

Kelley Dempsey
NIST IT Laboratory
Computer Security Division

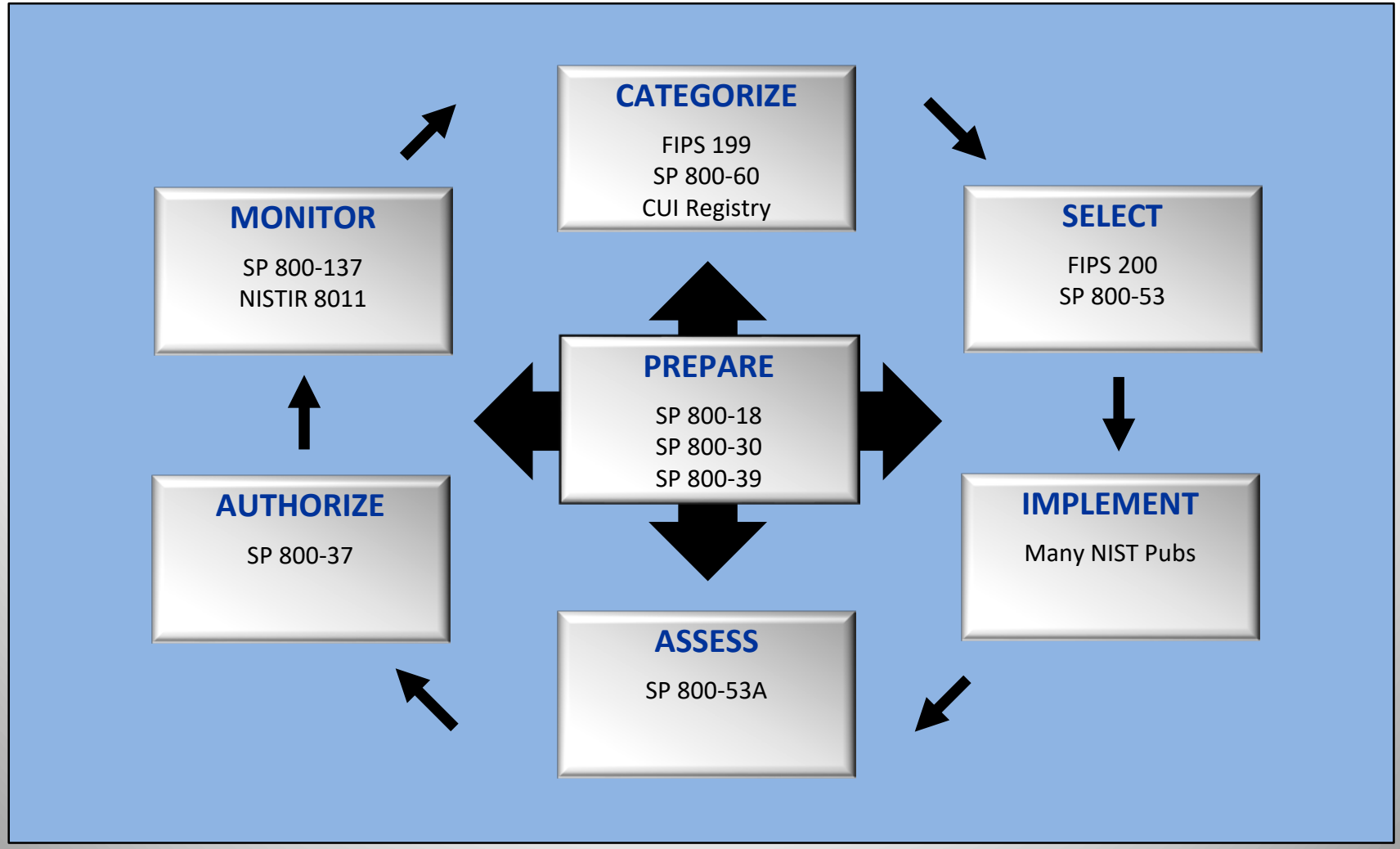
Naomi Lefkovitz
NIST IT Laboratory
Applied Cybersecurity Division

NIST SP 800-37 Revision 2

Risk Management Framework for Information Systems and Organizations

- Initial Public Draft released 9 May 2018
- Public comment period through 22 June 2018
- Final Public Draft planned for July 2018
- Final publication planned for October 2018

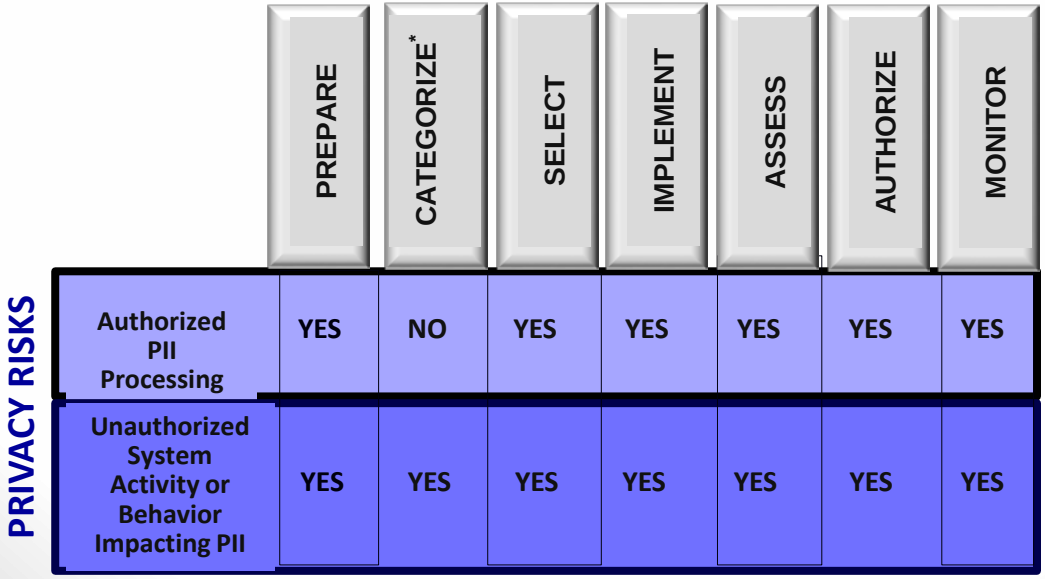
RMF 2.0


CATEGORIZE
FIPS 199
SP 800-60
CUI Registry
SELECT
FIPS 200
SP 800-53
IMPLEMENT
Many NIST Pubs
ASSESS
SP 800-53A
AUTHORIZE
SP 800-37
MONITOR
SP 800-137
NISTIR 8011
PREPARE
SP 800-18
SP 800-30
SP 800-39

RMF Improvements in Revision 2

- Addition of the organization and system level Prepare Step and associated tasks
- Integrates privacy risk management
- Expansion of Authorization options
- Aligns RMF with CSF
- Aligns RMF with security engineering processes
- Integrates supply chain risk management

Privacy Integration in Revision 2



* Except for system description, categorization tasks are not conducted to manage the risks arising from the authorized processing of PII.

Prepare Step Organization Level

- Task 1 – ID and assign people to RM roles
- Task 2 – Establish an org-wide RM strategy
- Task 3 – Assess org-wide risk
- Task 4 – Org-wide tailored baselines (optional)
- Task 5 – Common Control identification
- Task 6 – Prioritize within impact level (optional)
- Task 7 – Org-wide ISCM strategy

Prepare Step System Level (1 of 2)

- Task 1 – ID missions/business process to be supported
- Task 2 – ID interested stakeholders
- Task 3 – ID assets that require protection
- Task 4 – Determine authorization boundary
- Task 5 – ID information types

Prepare Step System Level (2 of 2)

- Task 6 – ID information lifecycle for PII (Naomi)
- Task 7 – Assess system-level risk
- Task 8 – Define protection needs and security and privacy requirements
- Task 9 – Determine placement within EA
- Task 10 – System registration IAW org policy

New/Revised Tasks in Existing Steps (1 of 2)

- Categorize, Task 2 – Review and approve categorization results and decision
- Select, Task 1 – Allocate requirements (expanded from ID common controls)
- Select, Task 3 – Tailor selected controls
- Select, Task 4 – Document planned implementation details in plans
- Implement, Task 2 – Document implementation details different from planned (config baseline)

New/Revised Tasks in Existing Steps (2 of 2)

- Assess, Task 1 – Select appropriate assessor
- Assess, Task 6 – POA&M (moved from Authorize)
- Authorize, Task 2 – Risk *analysis* added to risk determination
- Authorize, Task 3 – Respond to risk
- Authorize, Task 5 – Report the authorization decision and significant risk

Authorization Options

- Authorization to Operate
  - System Authorization (Traditional or Joint)
  - Type Authorization
  - Facility Authorization
- Common Control Authorization
- Authorization to Use
- Denial of Authorization

What Else is New? (1 of 2)

- Ongoing authorization supplemental guidance (June 2014) incorporated into Appendix F
- RMF and CSF alignment
  - Pre/postconditions reference CSF as applicable, e.g., CSF profile as potential output from Org Prep Task 4
  - Task Outcome tables reference CSF sections, categories, or sub-categories as applicable
  - References for each task list applicable CSF sections

What Else is New? (2 of 2)

- Security engineering process alignment
  - Task references list related 800-160 process as applicable
  - Section 2.3 discusses system elements/enabling systems and tasks focus on stakeholder requirements
- Supply Chain RM alignment
  - Discussion of Supply Chain Risk Management (SCRM) and the RMF added in section 2.6
  - SCRM addressed in Task discussions as applicable
  - SCRM artifacts included in task potential inputs and outputs as applicable
  - SCRM responsibilities noted in Appendix D

Contact Information

Project Leader and NIST Fellow

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

Senior Privacy Policy Advisor

Naomi Lefkovitz
(301) 975-2924
naomi.lefkovitz@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