Risk Management Framework (RMF) and Authority to Operate (ATO)

Tim Chick

Tom Scanlon

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Distribution Statements

Core DoD Policies and Governance

- Federal Information Processing Standards Publication 199 (FIPS-199)
- Committee of National Security Systems (NCSSI) 1253 – Categorization and Control Selection for National Security Systems
- Department of Defense Instruction (DoDI) 8500.01 - Establishes the positions of DoD principal authorizing official (PAO) and the DoD Senior Information Security Officer (SISO) and continues the DoD Information Security Risk Management Committee
- DoDI 8510.01 – Risk Management Framework for DoD Systems
  - Establishes the cybersecurity Risk Management Framework (RMF) for DoD Systems and establishes policy, assigns responsibilities, and prescribes procedures for executing and maintaining the RMF.
- National Institute of Standard and Technology (NIST) 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems

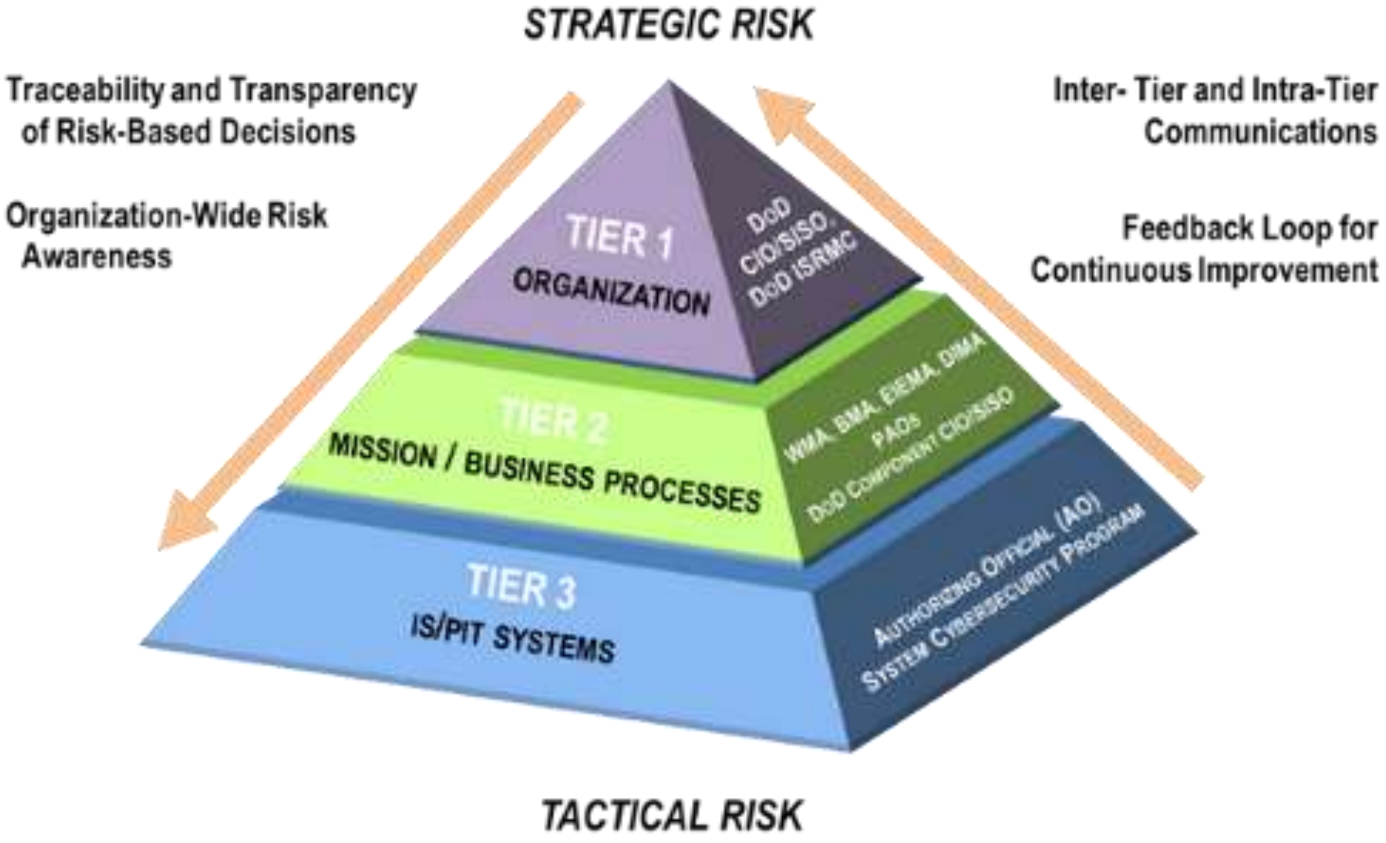
What is the Risk Management Framework (RMF)?

In 2014, the DoD started transitioning from the DoD Information Assurance Certification and Accreditation Process (DIACAP) to the Risk Management Framework for the DoD IT (RMF).

NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems", transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF).

The Risk Management Framework (RMF) provides a disciplined and structured process that integrates information security and risk management activities into the system development lifecycle.

DoD Risk Strategy


STRATEGIC RISK
Traceability and Transparency of Risk-Based Decisions
Organization-Wide Risk Awareness
Inter- Tier and Intra-Tier Communications
Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
DoD CIO/SISO, DoD ISRMC
TIER 2
MISSION / BUSINESS PROCESSES
WMA, BMA, EIEMA, DIMA
PAOs
DoD COMPONENT CIO/SISO
TIER 3
IS/PIT SYSTEMS
AUTHORIZING OFFICIAL (AO)
SYSTEM CYBERSECURITY PROGRAM
TACTICAL RISK

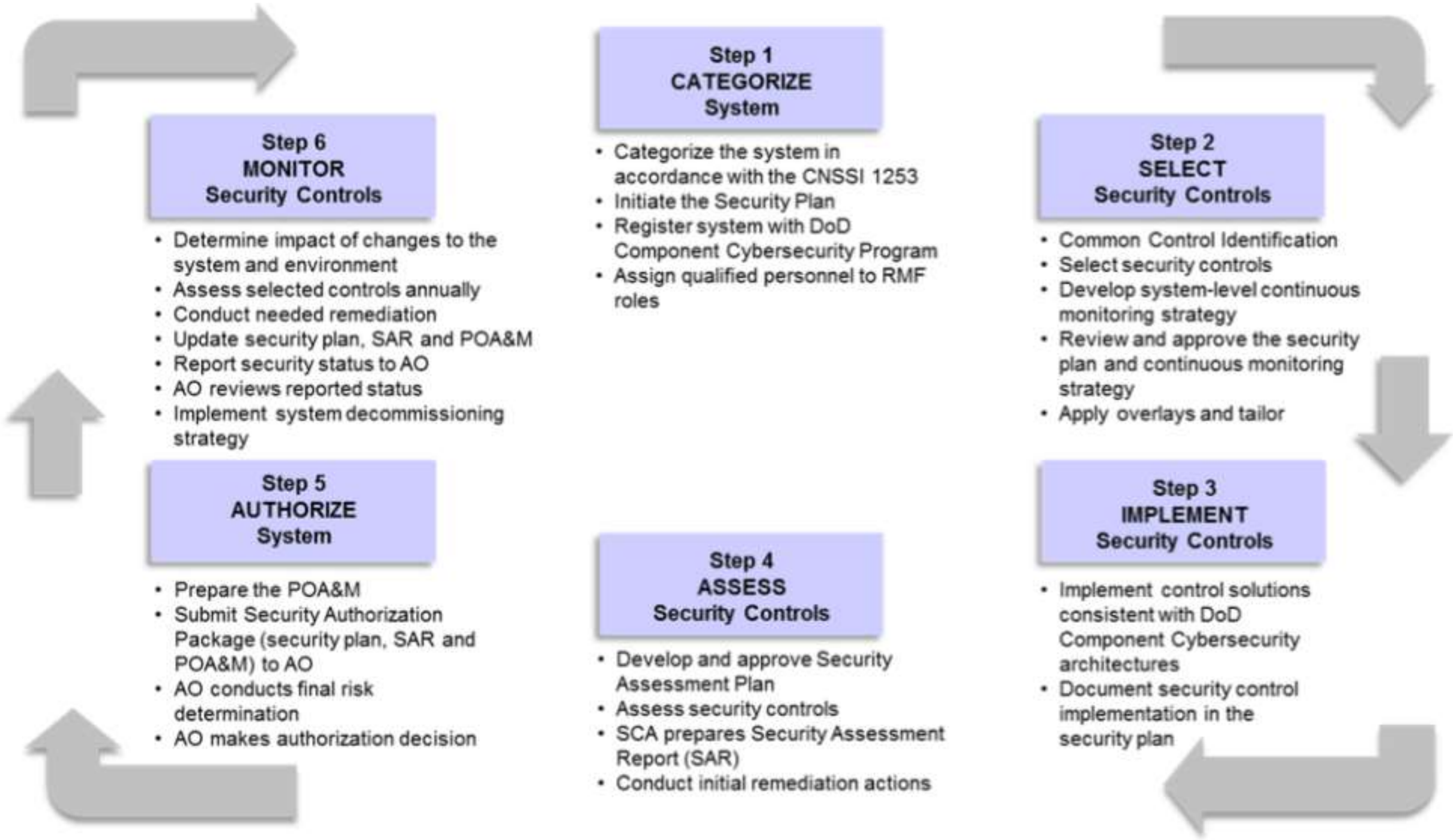
https://rmfks.osd.mil/rmf/PolicyandGovernance/Pages/GovernanceIntro.aspx

Authorizing Official (AO):

- Render authorization decisions for DoD Information Systems (IS) and Platform Information Technology (PIT) systems under their purview
- Establish guidance for and oversee IS-level risk management activities consistent with Commander, USSTRATCOM, and DoD Component guidance and direction.
- DoD officials with the **authority to assume responsibility formally for operating DoD ISs or PIT systems at an at an acceptable level of risk to organizational operations** (including mission, functions, image, or image, or reputation), organizational assets, individuals, other organizations, and the Nation.

DoDI 8500.01

The RMF Process



Step 1
CATEGORIZE
System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2
SELECT
Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT
Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4
ASSESS
Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

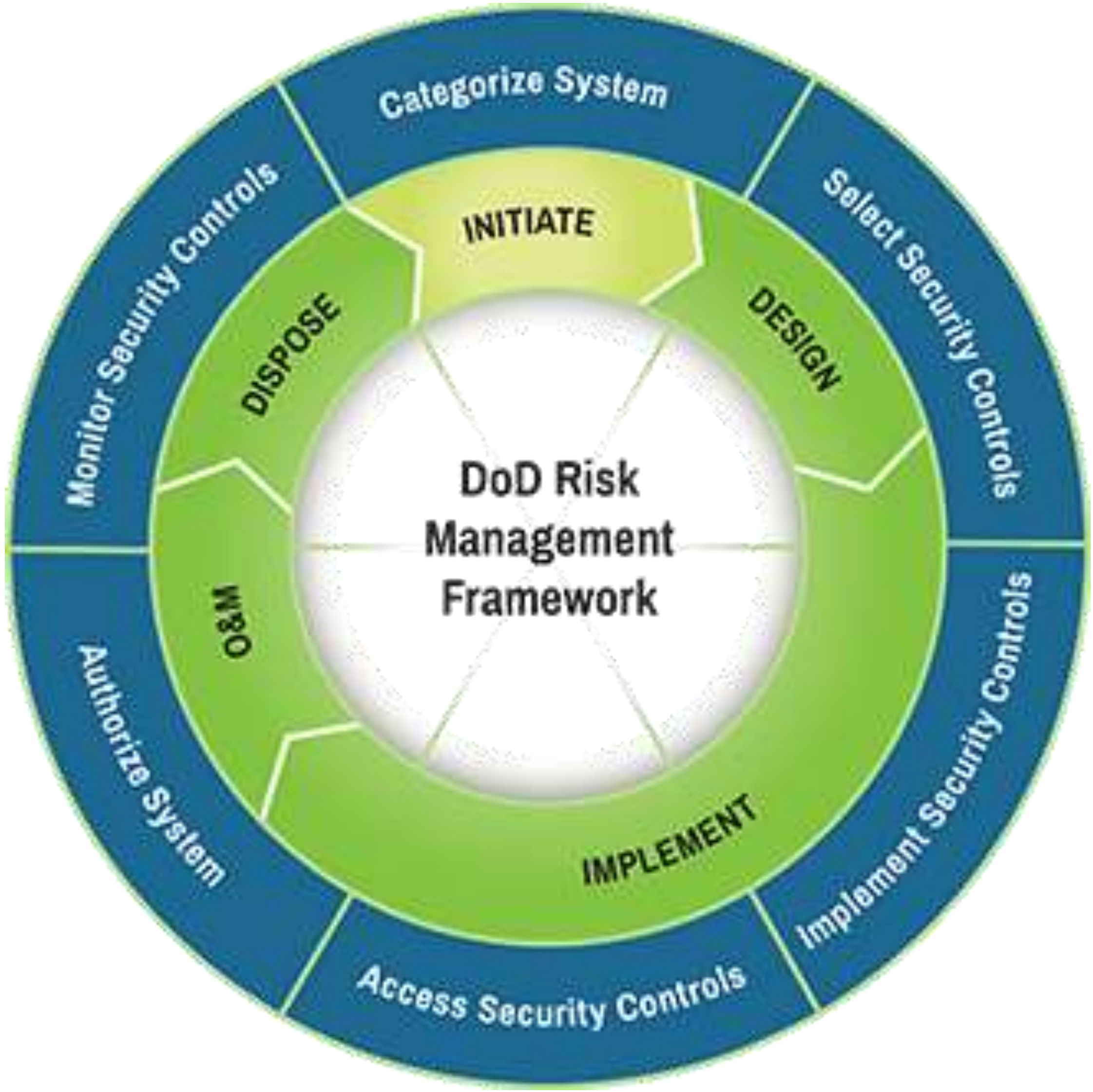
Step 5
AUTHORIZE
System

- Prepare the POA&M
- Submit Security Authorization Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6
MONITOR
Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

DoD System Lifecycle and RMF



http://www.truestonefed.com/wp-content/uploads/2016/09/risk-management-wheel.gif

The RMF/ATO Problem

Every system has **inherent risks** associated with it.

Program Manger (PM) is **graded** against the system's **KPP** and their compliance with all **regulations**, along with **cost** and **schedule** parameters.

PM makes **trades** between cost, schedule, quality, and functionality. With each trade **residual risks** occur.

Someone must **accept ALL residual risk** associated with the system before placing it into operations.

The Authorizing Official (AO) is responsible to **accepting information security risks**, which is done through the RMF process.

An ATO is usually good for 3 years, but **assumes no major changes** to the system's cybersecurity posture will be made during that time.

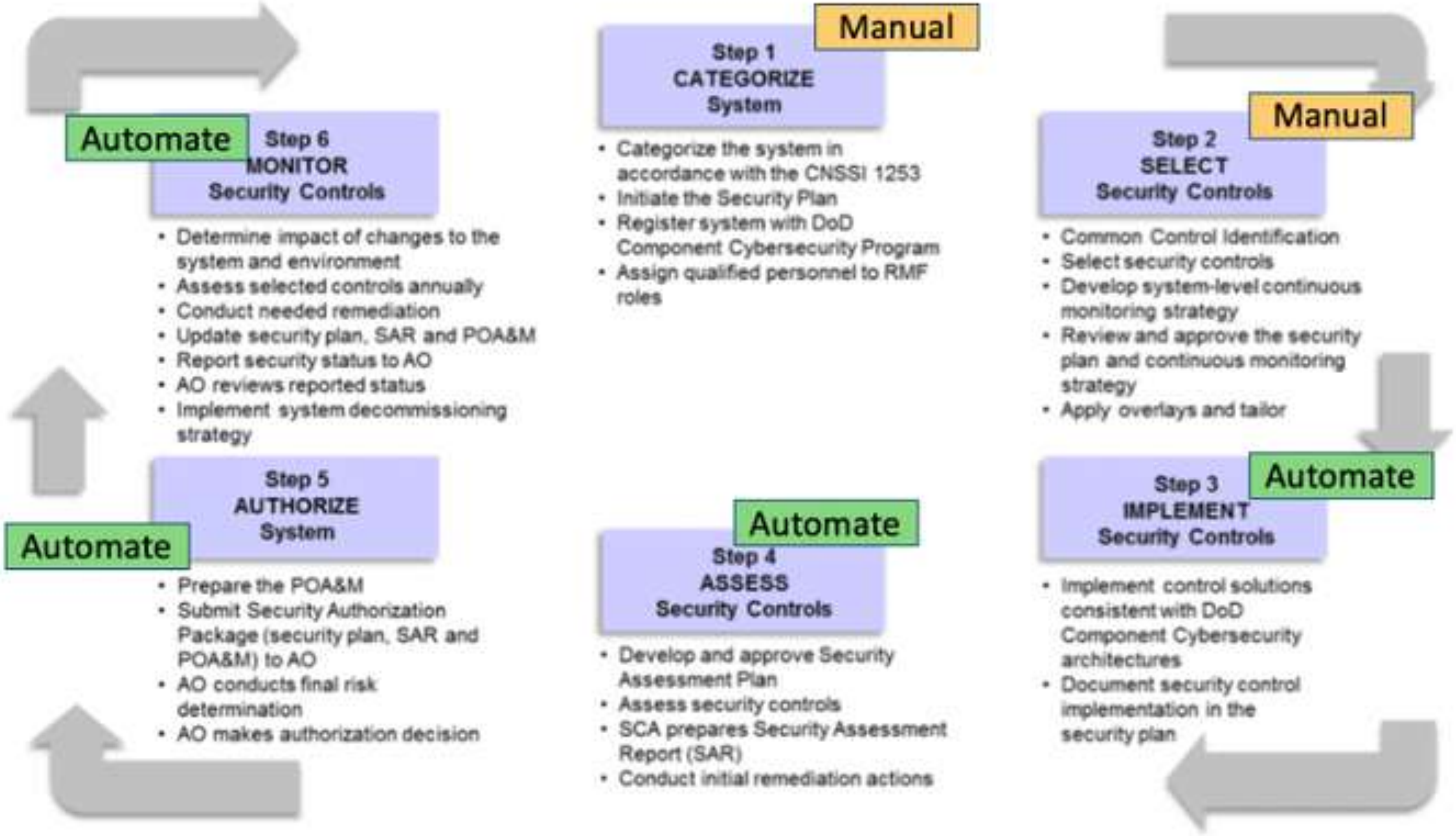
When **changes** do occur the AO may require a **reassessment** and **reauthorization**, which impacts the PM's cost and schedule and ability to deliver capability to the warfighter.

RMF’s Solution to Problem

RMF encourages an alternative approach to the traditional 3 year ATO process through ongoing authorization decisions or continuous reauthorization.

RMF assumes these systems have “been evaluated as having sufficiently robust system-level continuous monitoring programs”

The Goal



Manual

Step 1
CATEGORIZE
System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Manual

Step 2
SELECT
Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Automate

Step 3
IMPLEMENT
Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Automate

Step 4
ASSESS
Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Automate

Step 5
AUTHORIZE
System

- Prepare the POA&M
- Submit Security Authorization Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Automate

Step 6
MONITOR
Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Contact Information

Timothy A. Chick
tchick@sei.cmu.edu

Thomas P. Scanlon
scanlon@sei.cmu.edu

https://www.cylab.cmu.edu
https://s3d.cmu.edu
https://www.sei.cmu.edu