RMF TRAINING COURSES

Government-Developed Publicly Available Training Courses

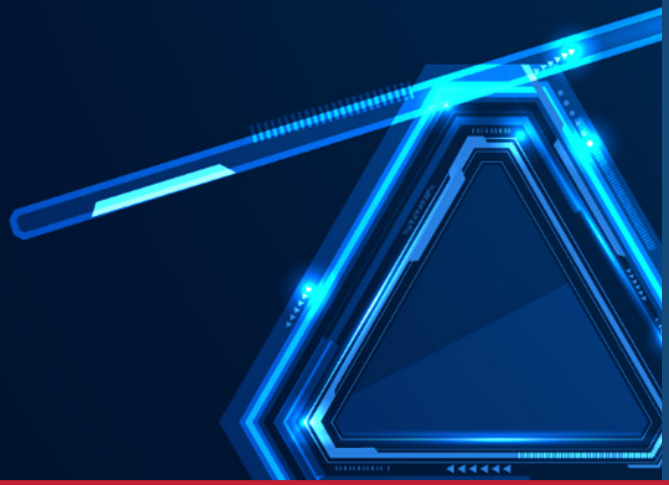
NIST: RMF for Systems and Organizations Introductory Course:

- This course describes at a high-level the importance of establishing an organization-wide risk management program, the information security legislation related to organizational risk management, the steps in the RMF, and the NIST publications related to each step.
- **https://csrc.nist.gov/projects/risk-management/rmf courses**

Center for Development of Security Excellence (CDSE): Introduction to the RMF:

- This course identifies policies and regulations that govern the Department of Defense (DOD) RMF process and defines DOD Information Technology and the categories of DOD information affected by the RMF.
- In addition, it provides an understanding of the seven step Implementation process of RMF and the RMF's applicability to the DOD Acquisition Process.
- **https://securityawareness.usalearning.gov/rmf/index.htm**

- Private training classes are also available from commercial vendors



ATO PROCESS KEYS TO SUCCESS

- Involve cybersecurity experts early

- Apply cybersecurity principles throughout the acquisition lifecycle
  - System design and architecture
  - Supply chain risk management
  - Software Assurance
  - Continuous monitoring

- Promote cybersecurity knowledge and best practices across career fields
  - It all starts with the contract and requirements
  - It is about risk management, not risk elimination
  - Use testing teams (blue, red, green, etc.) wisely and effectively
  - There is no substitute for proper oversight (Engineers, Logisticians, etc.)
  - Career field specific training is essential

ATOs FOR COMMERCIAL SYSTEMS

Commercial systems that connect to the DoD Information Network (DoDIN) or are utilized by DoD Components require both a DoD ATO and a DoD Program Manager. This Program Manager is part of a DoD Component that has a bonafide need for the system and will work with the vendor to obtain an ATO as part of the acquisition process. Integration of the RMF early in acquisition processes can potentially reduce the effort to achieve an ATO. Because a commercial system getting a DoD ATO is part of the acquisition process, it cannot begin without an interested DoD party.

For more information on cybersecurity in the DoD acquisition process please visit: **https://dodcio.defense.gov/Library/**

If you have any questions on the ATO process,

email the RMF Technical Advisory Group (TAG) Secretariat at:
osd.pentagon.dod-cio.mbx.rmf-tag-secretariat@mail.mil

ATO 101 FOR SMALL BUSINESSES

DOPSR 25-T-0014

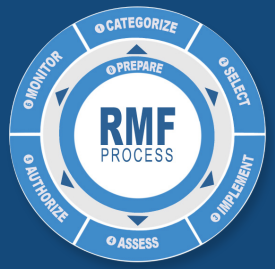
STANDARD ATO PROCESS

An **Authorization to Operate (ATO)** is an official approval that ensures a system's security and risk posture, compliance, and operation reflects an acceptable level of risk to the organization.

It utilizes the Risk Management Framework (RMF) which is essential in cybersecurity protocols for U.S. Federal Organizations. RMF is a step-by-step process to help manage and secure information systems. It involves:

- **Prepare** to execute the RMF from an organizational and system-level perspective by setting context and priorities for privacy and security risk management.
- **Categorize** the system and information to assign a risk category based on analysis of the information type, security requirements, and potential impact.
- **Select** appropriate security measures based on an initial baseline of security controls and appropriate tailoring based on an organizational assessment of risk.
- **Implement** security controls for these measures and describe how they are employed.
- **Assess** the controls to determine the extent they are implemented correctly, operating as intended and producing the desired outcome.
- **Authorize** the system to operate based on a determination of risk and the decision that this risk is acceptable.
- **Monitor** security controls on an ongoing basis and reporting the security state of the system to designated organizational officials.

This framework provides the capability to manage system-related security risks more effectively in diverse environments of complex and sophisticated cyber threats and ever-increasing system vulnerabilities.



ASSESS ONLY

While all systems require ATOs, the DoD created the **"Assess Only"** construct, which allows organizations to incorporate and use products and services that fall below the system level (e.g., system components, hardware, software, IT services) without going through the full ATO process.

HARDWARE

The DoD defines hardware as devices or products with embedded software, often referred to as firmware (e.g., hardware with wireless capabilities, network devices, controllers, and sensors).

These technologies are assessed against a defined assessment process and then incorporated into an existing authorization boundary as part of the larger system's authorization baseline (e.g., network router, firewall, server) and are re-assessed as necessary and authorized as part of the system.

SOFTWARE

The DoD defines this as software independent of an operating system that will be incorporated into a system boundary. Such products are assessed using Security Technical Implementation Guides (STIGS), vulnerability scans, and analysis of applicable Information Assurance Vulnerability Alert (IAVA) compliance.

Software can be:

- Commercial-off-the-shelf (COTS)
- Government-off-the-shelf (GOTS)
- Mobile applications
- Open-source software items

ASSESSMENT PROCESS

- **Risk Assessment:** Approved assessor determines the level of risk associated with the technology
- **Implement:** Applicable security controls identified in the assessment are implemented
- **Risk Acceptance:** Assessment results made available; system RMF package is updated
- **Monitor:** Monitor per system continuous monitoring plan

CLOUD (SaaS)

Cloud Service Providers (CSPs) are granted an Authorization to Operate (ATO) primarily for enterprise use. CSPs may obtain a Federal Risk and Authorization Management Program (FedRAMP) or DoD authorization for their Cloud Service Offerings (CSOs):

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

The authorization process for commercial and non-commercial CSPs is based on Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) A-130, National Institute of Standards and Technology (NIST) RMF processes leveraging FedRAMP, and the FedRAMP Authorization Act, supplemented with agency-specific considerations.

CSPs must comply with all continuous monitoring requirements to maintain the ATO (e.g., vulnerability solutions/mitigation requirements and annual assessments).

- FedRAMP Page on Agency Authorization: **https://www.fedramp.gov/agency-authorization/**
- DoD Cloud Computing Security Page: **https://public.cyber.mil/dccs/**

For more information on the ATO process, visit:
https://csrc.nist.gov/Projects/risk-management

https://www.nist.gov/itl/smallbusinesscyber

https://csrc.nist.gov/pubs/sp/1314/final