Improving Cybersecurity Through the Implementation of the DoD Risk Management Framework

Presented by Gerald Blondeaux

October 8, 2014

TASC
INSIGHT APPLIED™

Risk Management Framework (RMF) Overview

- DoDI 8500.01: Cybersecurity
- DoDI 8510.01: RMF
- DoD Information Technology (IT) Overview
- RMF Lifecycle
- RMF Governance: Three Tier Approach
- RMF Alignment with DoD Acquisition Process
- Closing: Improve Cybersecurity Through RMF
- References

DoDI 8500.01: Cybersecurity

Ensures **Mission Risk and Mission Resilience** are **Central to Program** and operational decisions.

Cybersecurity Applicability

Applicable to all IT that interacts with DoD information by:

- Receiving
- Processing
- Storing
- Displaying
- Transmitting

Including weapons systems and industrial control systems.

No Anonymity

Applicable to every DoD organization and all DoD information regardless of where information resides.

Enterprise-Wide Cybersecurity Solutions

Gain efficiencies through "build once, use many" cybersecurity approach through centrally built, hosted, and authorized capabilities in DoD networks.

DoD Alignment

Aligns DoD with federal government by adopting NIST and CNSS standards.

Increased Product Availability

Vendors may now build products once in accordance with NIST guidelines. This improves deployment across all government agencies saving development time and costs and fosters reciprocity between agencies.

Promote Sharing

Similar products across agencies improves operating knowledge base while promoting interoperability and information sharing.

DoDI 8510.01: RMF

Emphasizes **Information Security & Continuous Monitoring** with timely correction of deficiencies.

Tiered Approach to Risk Management

Implements a three-tiered approach to risk management that address risk-related concerns at the enterprise level, mission and business process level, and information level.

Synchronize

Three-tier approach to cybersecurity risk management synchronizes and integrates across all levels and phases of IT.

Risk Management Methods

Provides organizations an accurate status of vulnerabilities caused by non-compliant controls with relation to other risk factors including threat, impact, and likelihood.

Buy Down Cybersecurity Risk

Focuses on risks incurred by missions and how to buy down cybersecurity risks through applying the most effective and appropriate mitigations.

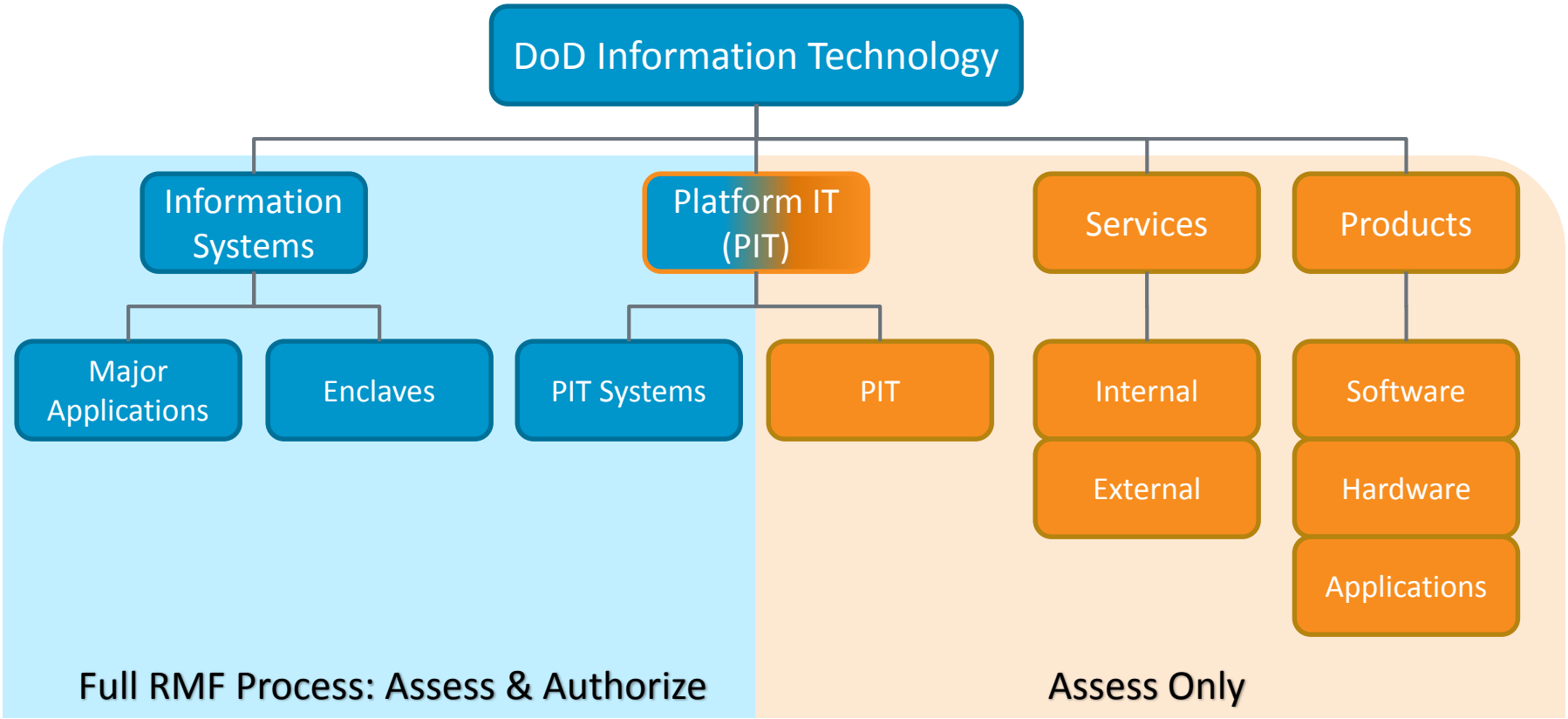
Establish Reciprocity

Organizes system authorization reciprocity, enabling agencies to accept approvals by other agencies for interconnection or reuse of IT without retesting.

Reduce Cost

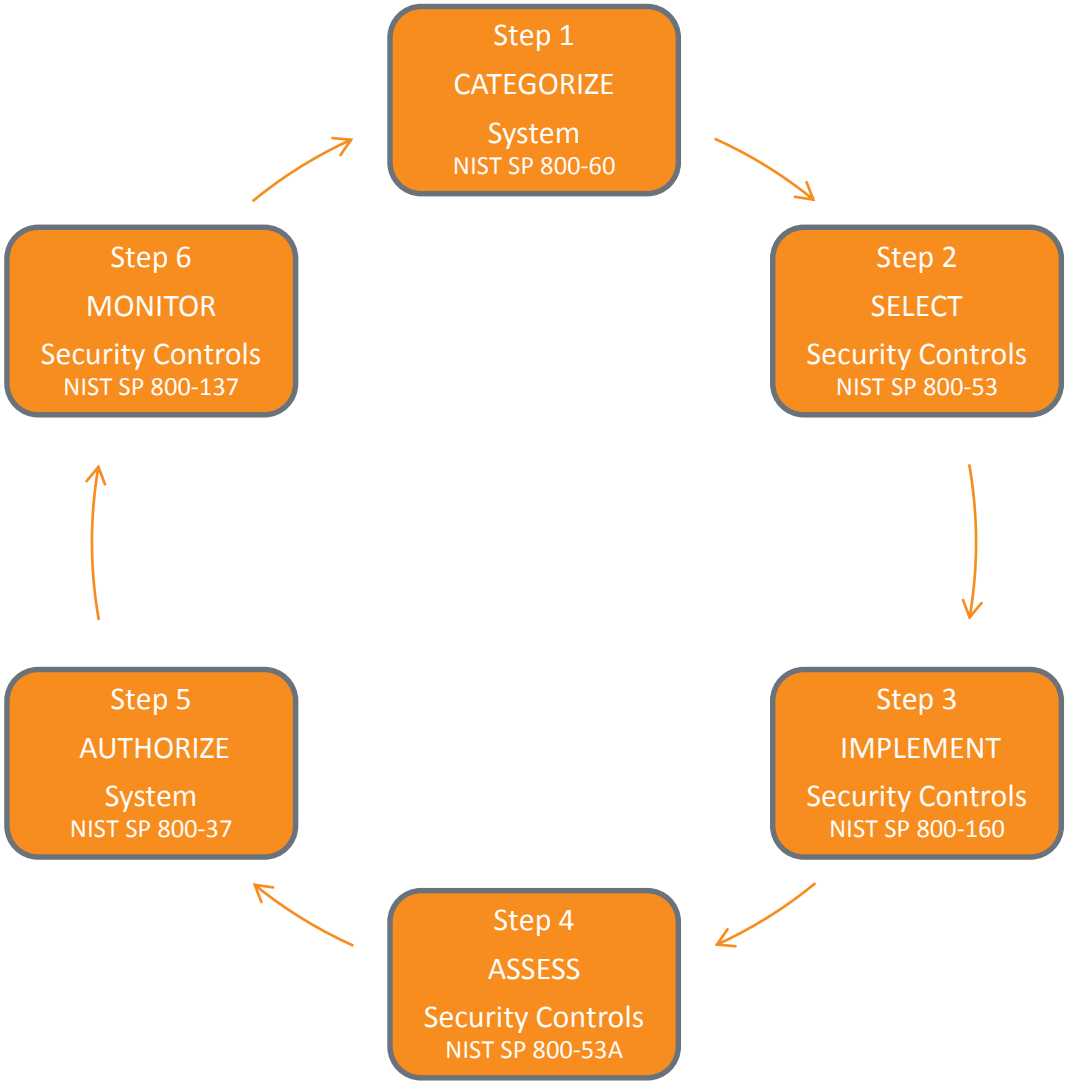
Reciprocity reduces the schedule and financial impacts associated with testing and retesting systems that otherwise have minimal impact to security.

DoD Information Technology Overview



RMF Applies to All Information Technology

RMF Lifecycle



RMF Lifecycle Step 1: Categorize System

Categorize System

Early cybersecurity consideration determine impact:

- For information **processed, stored, transmitted, or protected by the information system**
- For the information system

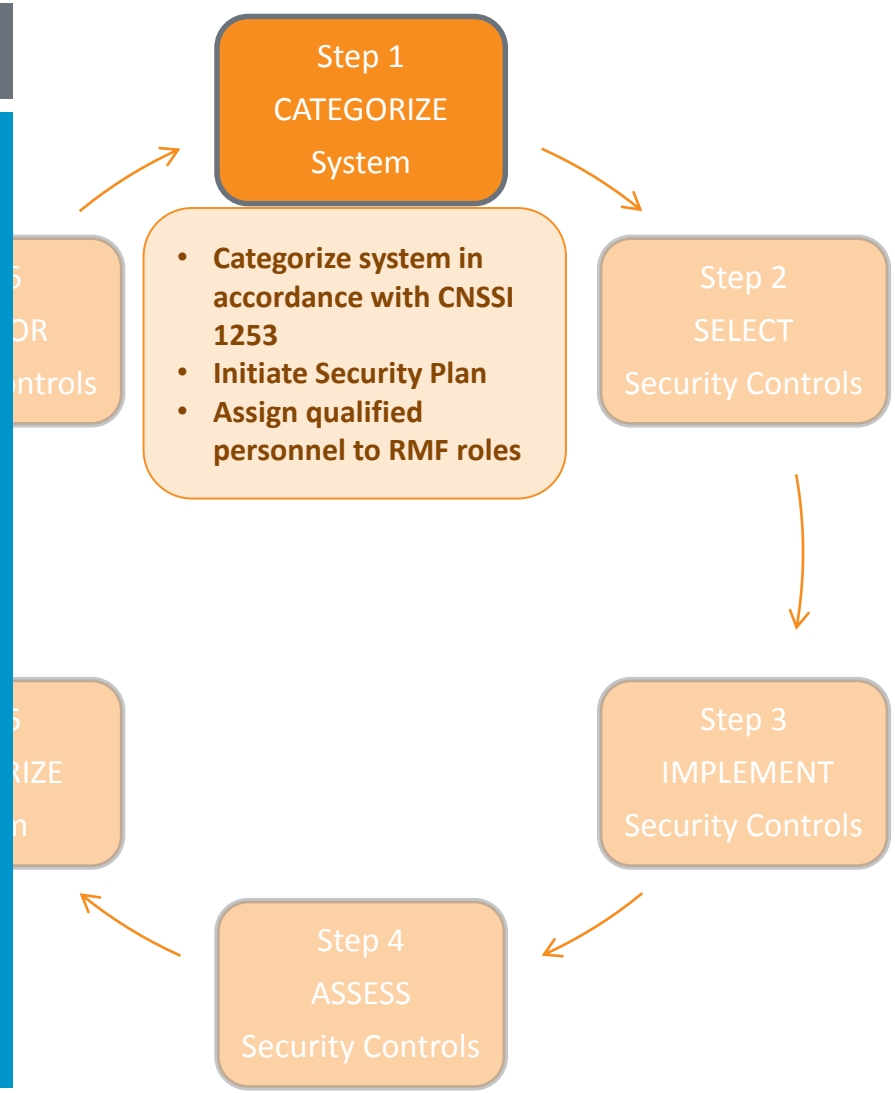
NIST SP800-60 V. II provides impact values for various information types.

Security objectives include:

- Confidentiality
- Integrity
- Availability

Impact values applied to each security objective are:

- Low
- Moderate
- High



RMF Lifecycle Step 2: Select Security Controls

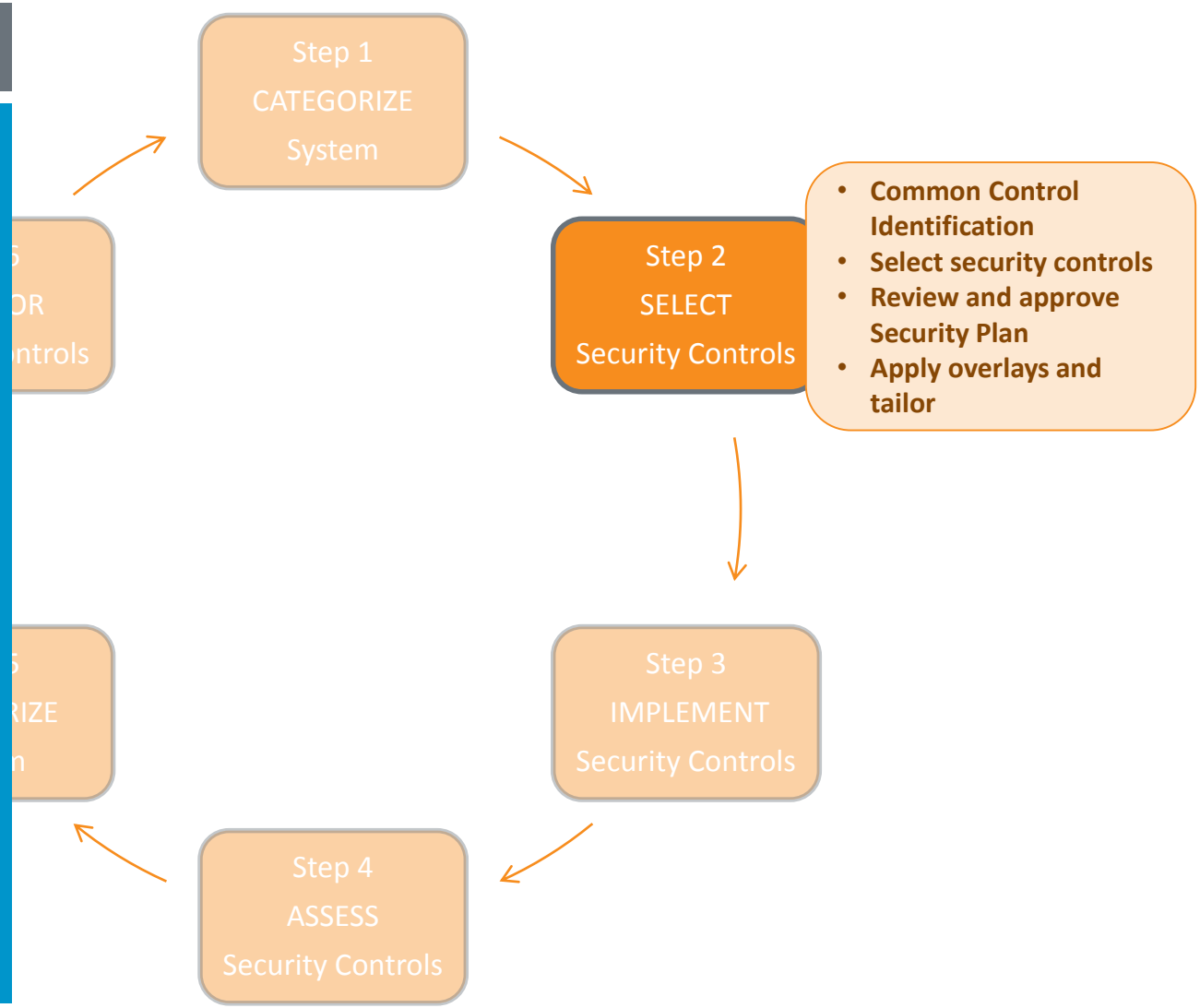
Select Security Controls

Select the **initial security controls**

- Select baseline controls from CNSSI 1253 based on the security category
- Apply overlays identified during security categorization

Tailor the initial security controls

- Identify and designate common controls, apply scoping considerations, select compensation controls, assign specific parameter values, and supplement baselines based on risk assessment
- Determine if additional assurance–related controls are required to increase the level of trustworthiness in the information system and supplement as needed

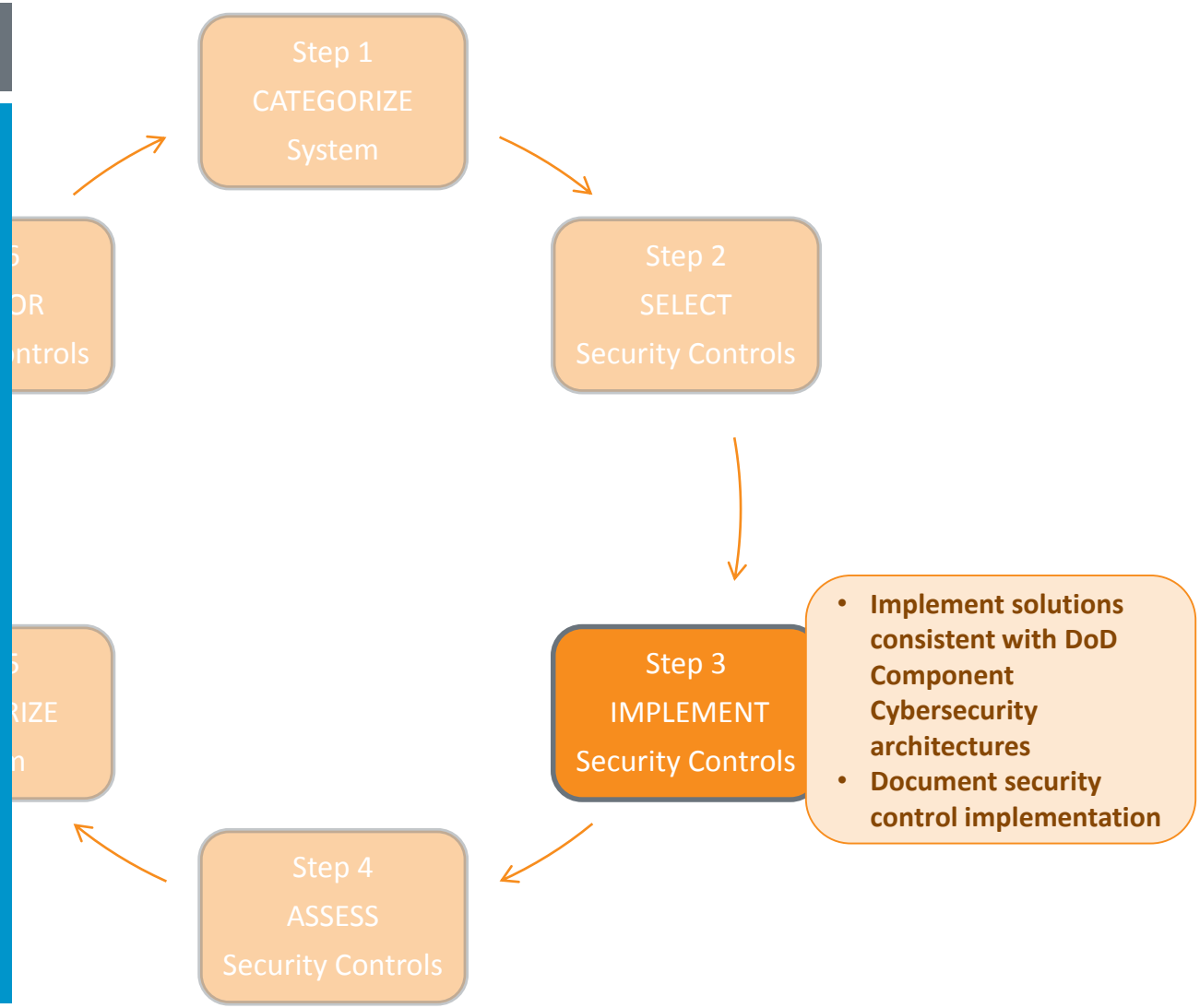


RMF Lifecycle Step 3: Implement Security Controls

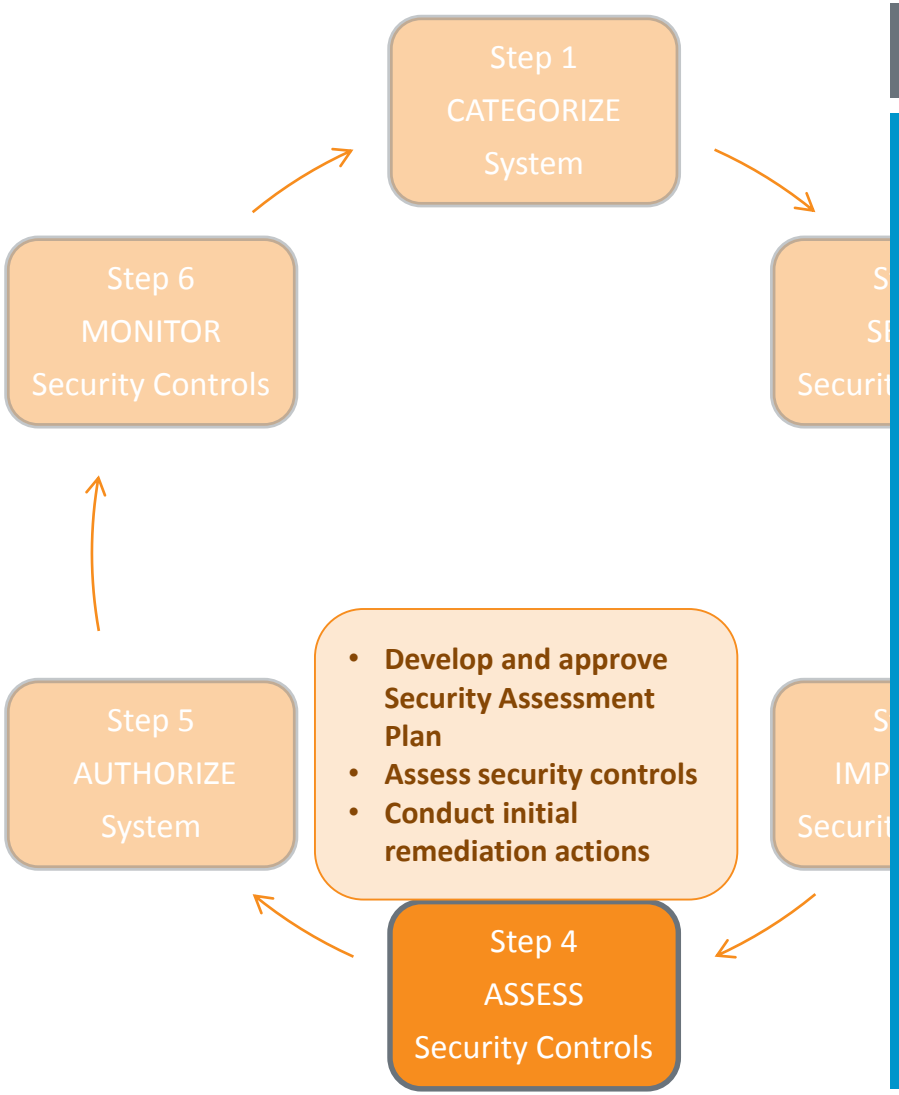
Implement Security Controls

Implement security controls from security plan following DoD guidance found on the RMF Knowledge Service.

- Apply STIGs or SRGs when STIGs are not available
- **Early and consistent involvement with security engineers**
- Address system security design in preliminary and critical design reviews
- **Document security control implementation in the security plan with implementation description per RMF KS**
- Identify and associate compliance for security controls that are inherited by IS and PIT from hosting or connected system



RMF Lifecycle Step 4: Assess Security Controls



Assess Security Controls

Develop and approve a security control assessment plan.

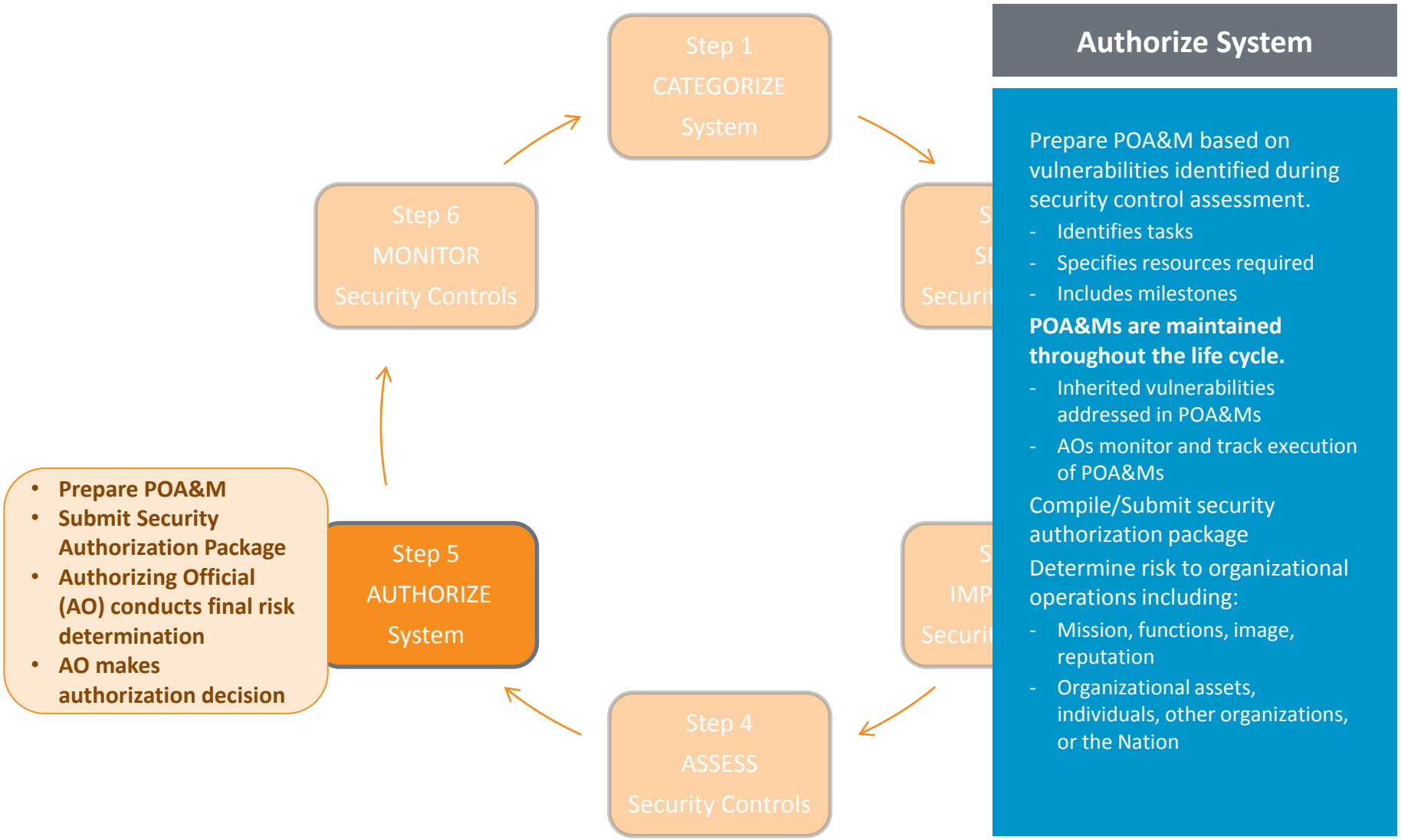
- Coordinate security control assessment with all other acquisition process test events
- **Document coordination to maximize synergy support reciprocity and reduce retesting**

Assess security controls per assessment plan.

- Record security control compliance *status*
- Assign vulnerability severity value for security controls
- Determine risk level for security controls
- Assess and characterize aggregate level of risk to the system

Conduct remediation actions on noncompliant security controls.

RMF Lifecycle Step 5: Authorize System



Authorize System

Prepare POA&M based on vulnerabilities identified during security control assessment.

- Identifies tasks
- Specifies resources required
- Includes milestones

POA&Ms are maintained throughout the life cycle.

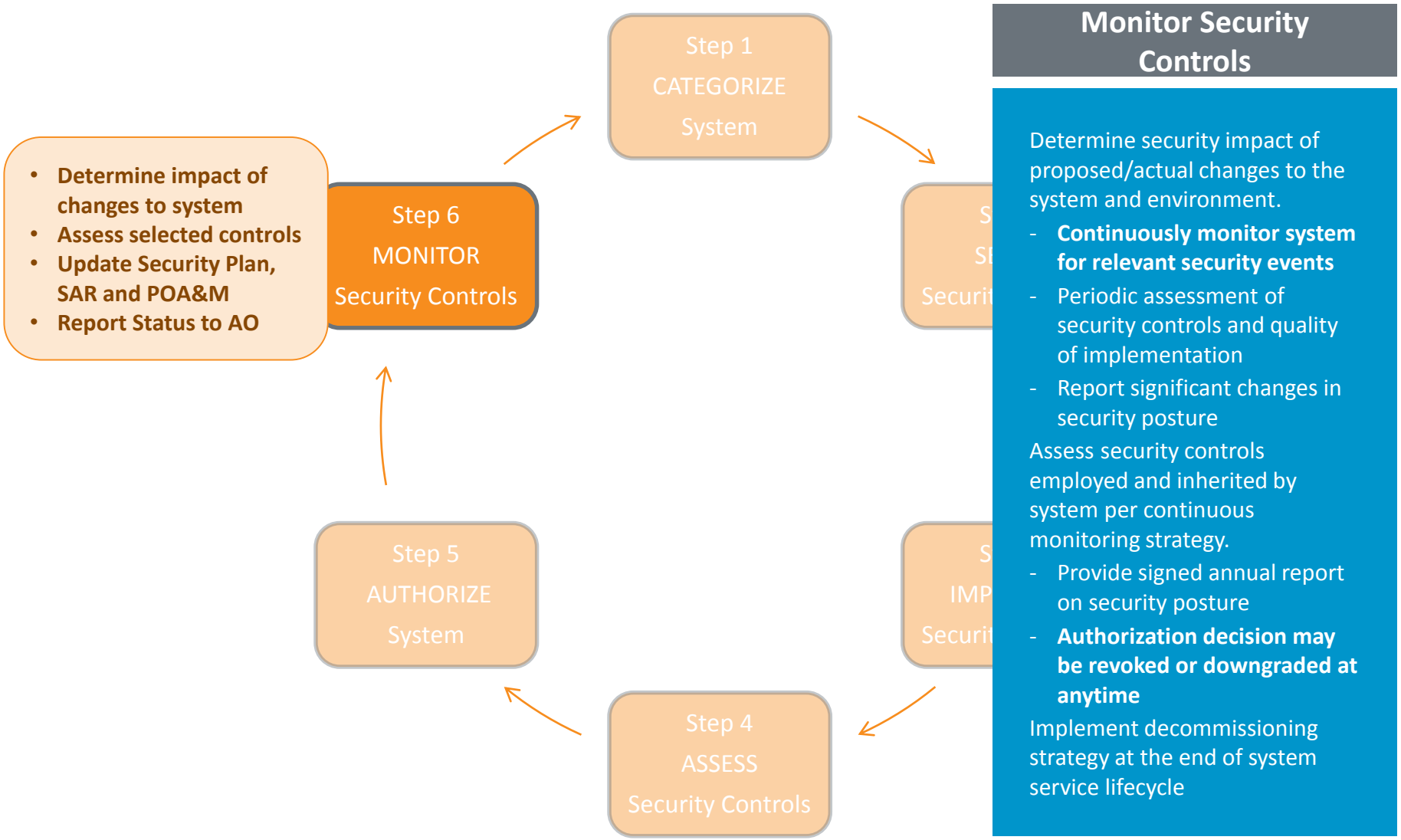
- Inherited vulnerabilities addressed in POA&Ms
- AOs monitor and track execution of POA&Ms

Compile/Submit security authorization package

Determine risk to organizational operations including:

- Mission, functions, image, reputation
- Organizational assets, individuals, other organizations, or the Nation

RMF Lifecycle Step 6: Monitor Security Controls



Monitor Security Controls

Determine security impact of proposed/actual changes to the system and environment.

- **Continuously monitor system for relevant security events**
- Periodic assessment of security controls and quality of implementation
- Report significant changes in security posture

Assess security controls employed and inherited by system per continuous monitoring strategy.

- Provide signed annual report on security posture
- **Authorization decision may be revoked or downgraded at anytime**

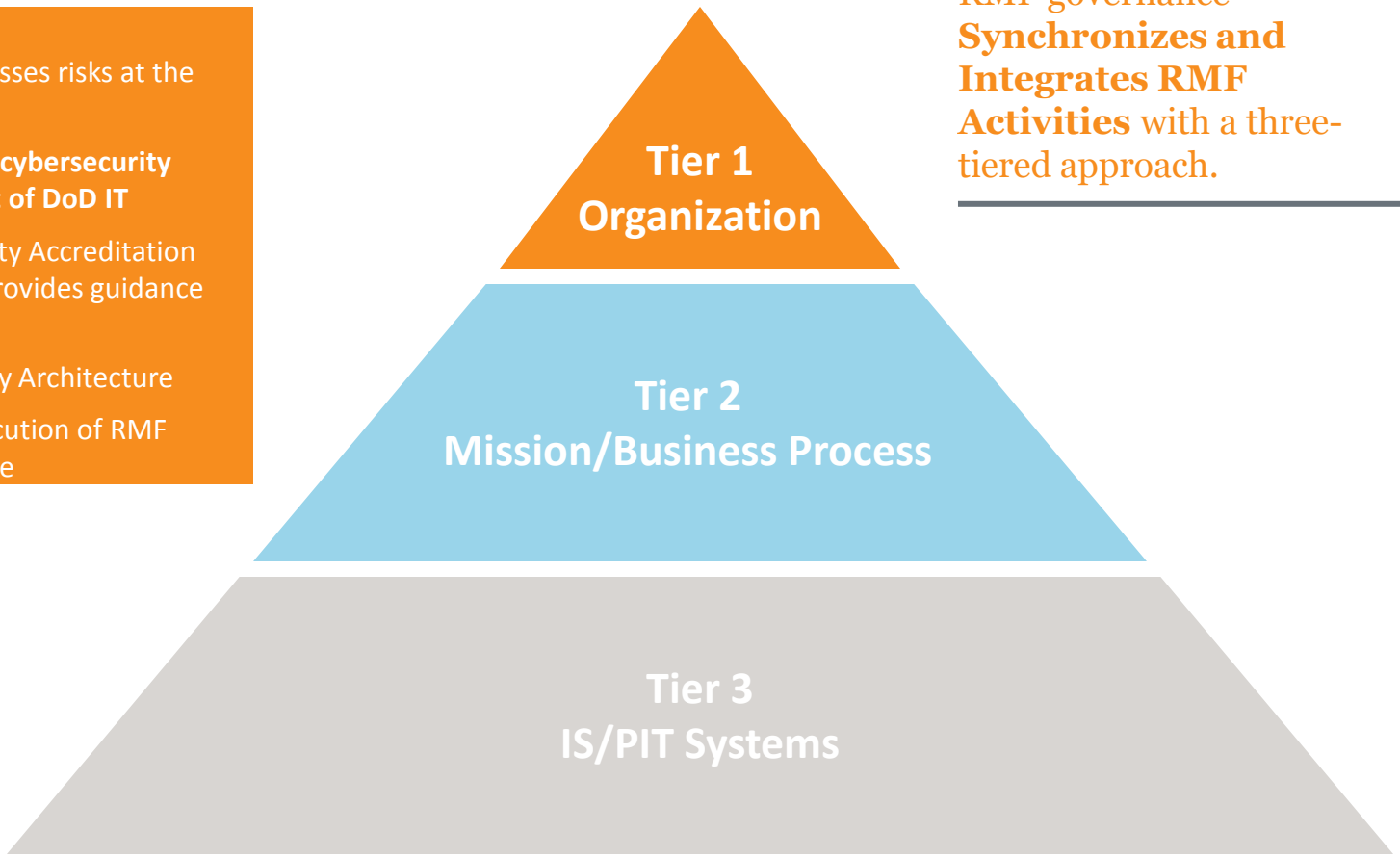
Implement decommissioning strategy at the end of system service lifecycle

RMF Governance: Three Tier Approach

Tier 1

Strategic level addresses risks at the enterprise level.

- **Directs/oversees cybersecurity risk management of DoD IT**
- Defense IA Security Accreditation Working Group provides guidance to AOs.
- DoD Cybersecurity Architecture
- Planning and execution of RMF Knowledge Service



RMF governance **Synchronizes and Integrates RMF Activities** with a three-tiered approach.

RMF Governance: Three Tier Approach

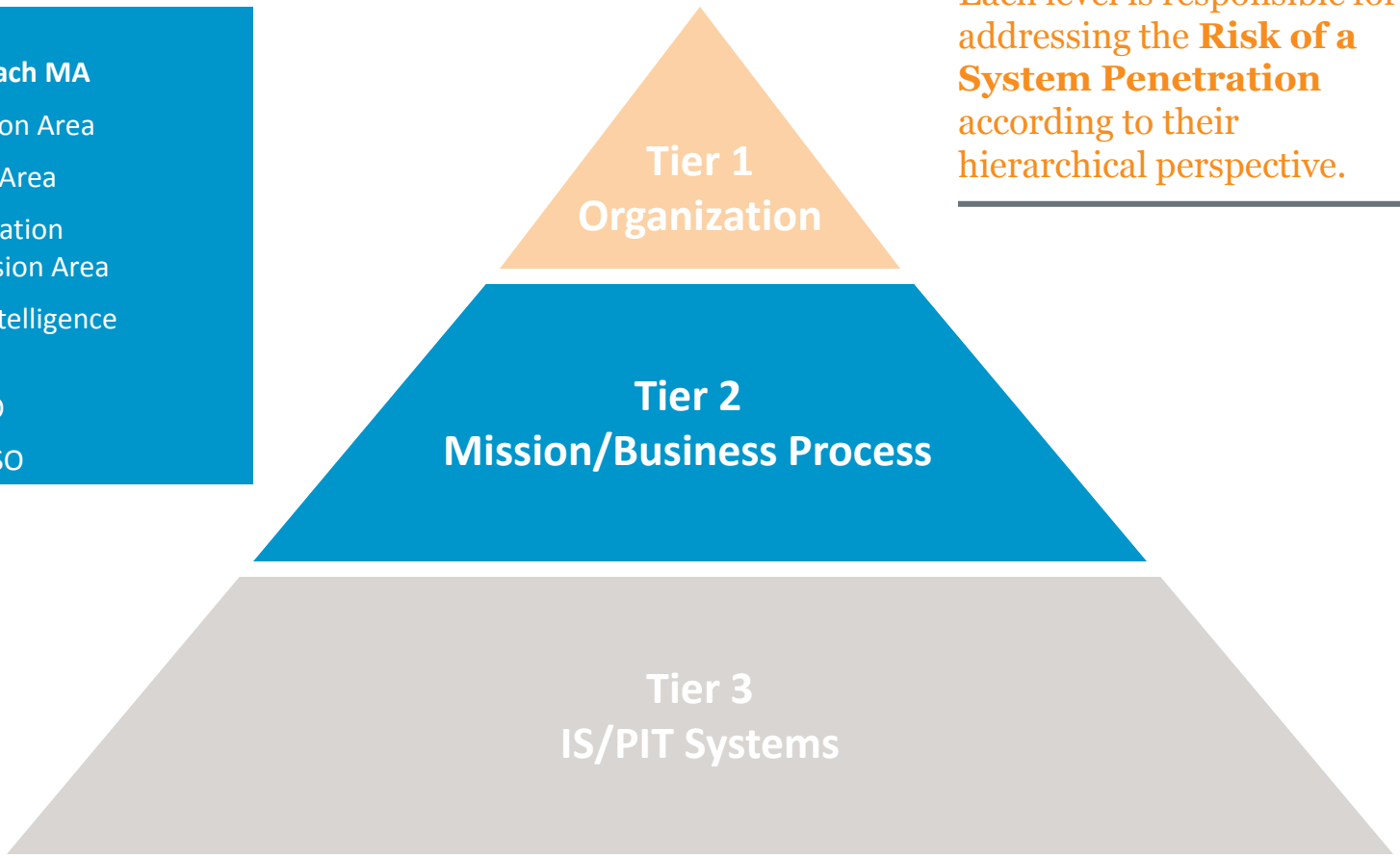
Tier 2

PAO appointed to each MA

- Warfighting Mission Area
- Business Mission Area
- Enterprise Information Environment Mission Area
- DoD Portion of Intelligence Mission Area

DoD Component CIO

DoD Component SISO



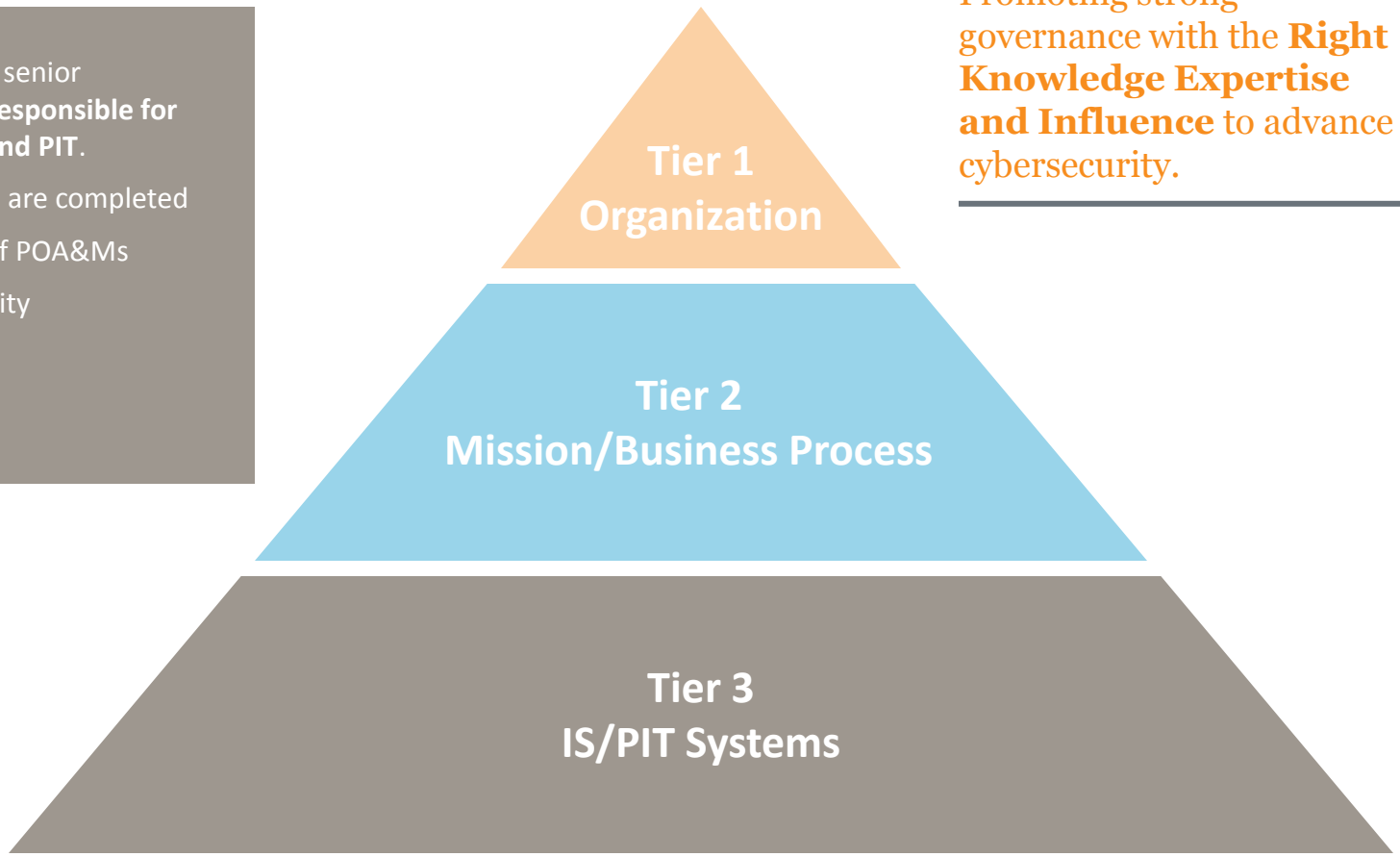
Each level is responsible for addressing the **Risk of a System Penetration** according to their hierarchical perspective.

RMF Governance: Three Tier Approach

Tier 3

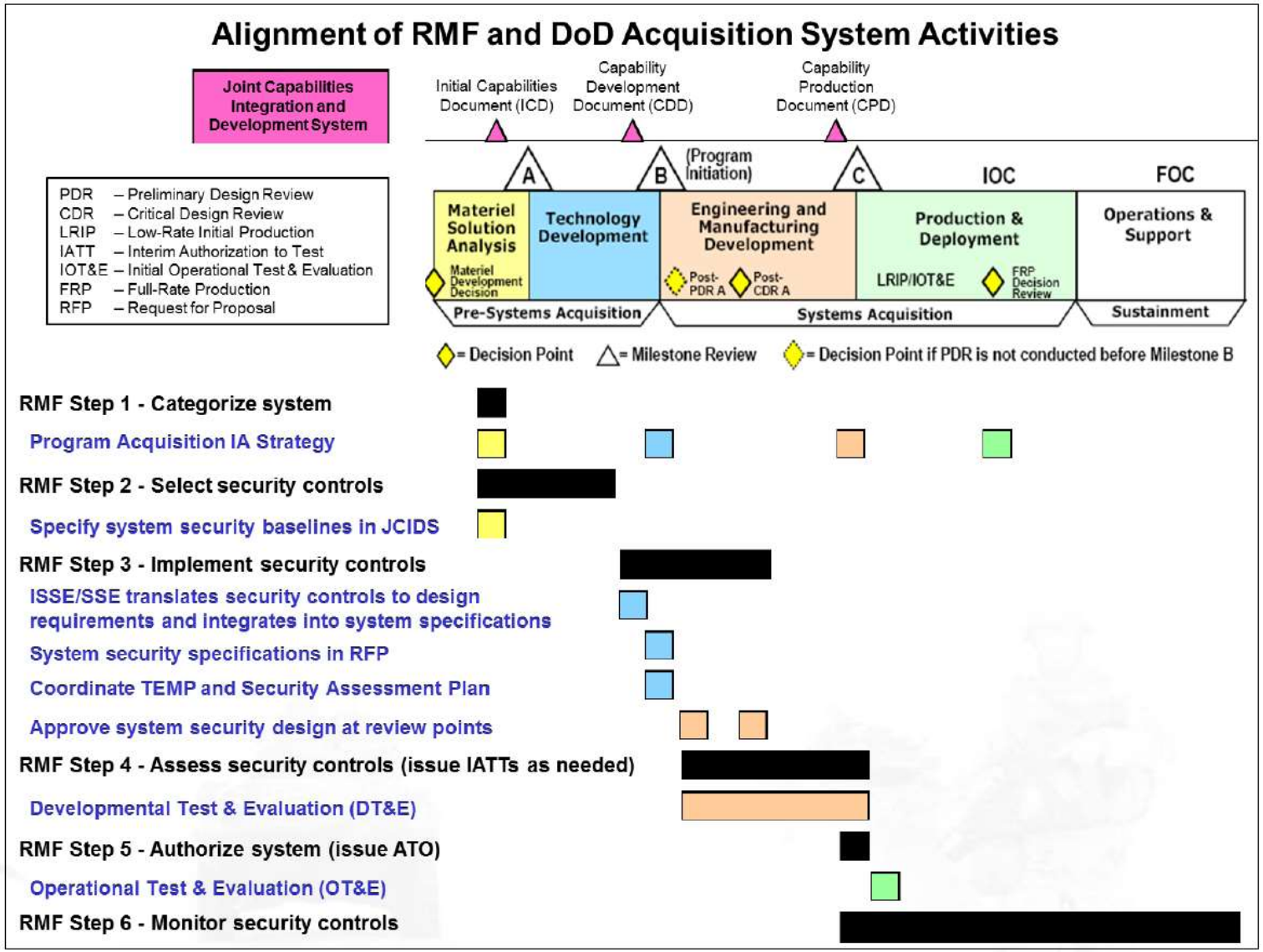
AOs are assigned by senior leadership and **are responsible for their respective IS and PIT**.

- Ensure RMF tasks are completed
- Track execution of POA&Ms
- Promote reciprocity



Promoting strong governance with the **Right Knowledge Expertise and Influence** to advance cybersecurity.

RMF Alignment with DoD Acquisition Process



Consistently applied across the acquisition life cycle.

Closing: Improve Cybersecurity Through RMF

- Aligns defense and federal civilian cybersecurity guidance
- Applicable to all IT
- Early and consistent approach to cybersecurity
- Common framework, security controls
- Clearly defined milestones within the acquisition process
- Enables and supports reciprocity
- Reduce time and costs associated with redundant testing

Policy References

Title	Purpose	Link
Knowledge Service	DoDI 8510, Authoritative Guidance	https://rmfks.osd.mil/
DISA IA Support Environment	STIGs, CCIs, SRGs, DAA/AO Training	https://iase.disa.mil/index2.html
CNSS Policies	CNSSI 1253, Security Control Categorization and Selection	https://www.cnss.gov/policies.html
NIST Publications	NIST SP 800-53 Rev. 4 Security Controls, NIST SP 800-37, Guide to implementing RMF	https://csrc.nist.gov/publications/PubsSPs.html
Risk Management Framework for DoD Information Technology	DoDI 8510.01	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
Cybersecurity	DoDI 8500.01	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

Thank you

For more information, contact

Gerald Blondeaux
gerald.blondeaux@tasc.com
520 275 0557

TASC
INSIGHT APPLIED™