Headquarters U.S. Air Force

Integrity - Service - Excellence

Risk Management Framework (RMF) Next

U.S. AIR FORCE

Capt Jacob T. Mireles
SAF/CIO A6Z
28 Aug 2018

Agenda

- What is RMF Next
- Current RMF Challenges
- CyberWorx
- RMF Next Scope
- Foundational Pillars
- Guidance
- Approach
- Outcomes
- Next Steps

RMF Next

RMF Next is the initiative to apply design thinking to the implementation of the RMF with the objective of implementing risk management in a manner that:

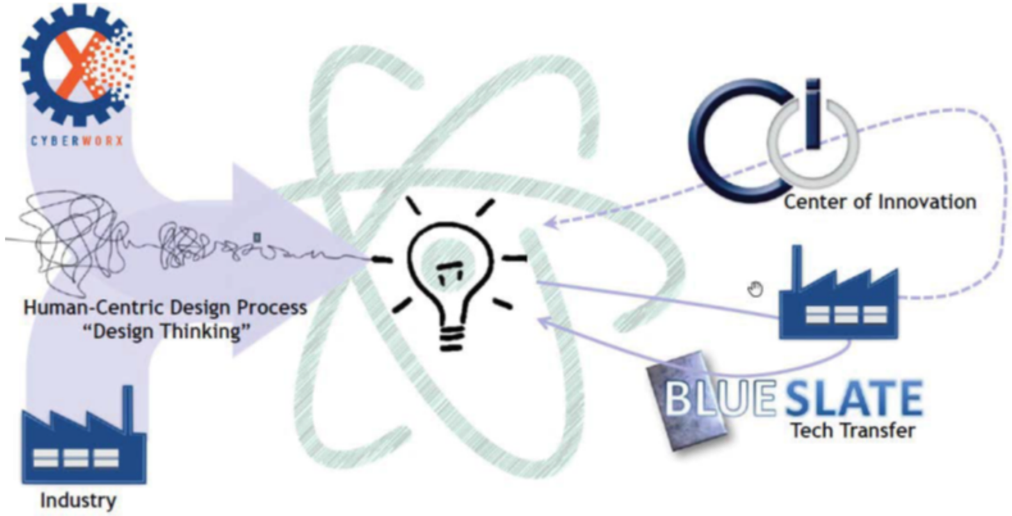
- **Supports innovation by shortening the dev-to-warfighter timeline**
- **Maximizes reciprocity and inheritance policies**
- **Develops an enterprise risk management methodology**

Current RMF Challenges

- Threat Integration
  - Make decisions based on threat
- Risk Decision Maker
  - Is it the AO, mission owner, mission area owner, all/none?
- Inconsistency of Implementation
  - Every AO has developed their own risk model
- Skills Gap and Training
  - What is required to perform the roles (NICE Framework)
  - Having a certification is not enough
- Culture: Security must be a priority

Cyberworx

- Cyberworx Design Think vs. Lean Six Sigma Process Improvement
  - Not focused on looking at the current process
  - Complete redesign using Discovery and Ideation Cyberworx process
  - Includes Voice of the Customer (VOC) – the Warfighter
  - Discovery event held at Scott AFB, January 2018
  - Design Sprint Event held at USAFA, April 2018
- Pain Points
  - Inaccurate security posture
  - No consistency
  - Laborious
  - Considered a hindrance

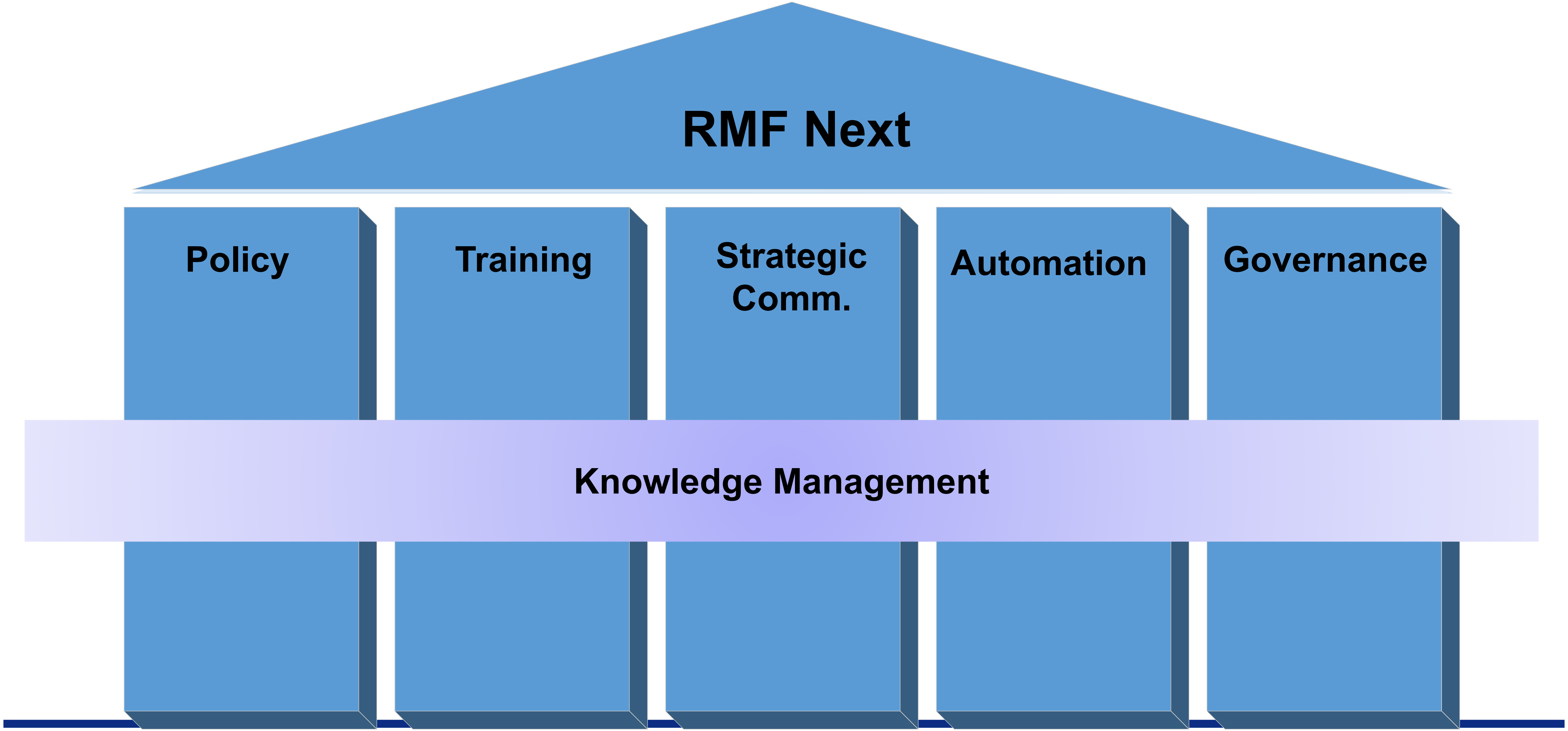


Use Case's

Use Case Teams were established by utilizing prior CyberWorx working group

- Team # 2 – Migrate to the Cloud
- Team # 3 – Software as a Service (SaaS)
- Team # 4 – Cyber Defense System
- Team # 5 – Industrial Control Systems
- Team # 6 – Enclave System
- Team # 8 – Education and Training Systems

Foundational Tenants



Guidance

- Leverage new NIST SP 800-37 Revision 2
  - Links Tier 1 and Tier 3 better
  - Step “0” Prepare
  - Cybersecurity Framework
  - Privacy Risk Management
  - SecDevOps
  - Supply Chain Risk Management (SCRM)
  - Alternative Control Selection

Approach

- Prepares the organization to manage security and privacy risks
  - Tier 1 and Tier 3
- Each foundational team consisted of members from SAF and across the MAJCOMs
- Weekly SAF and bi-weekly team meetings ensured collaboration of stakeholders
- Analyze Step – 0 Tasks and Outcomes
- Leverage the “Foundational Tenets” to identify deliverables to enable “Outcome”
  - Tier 1 – USAF Organization Prospective
  - Tier 3 – USAF System/Use Case Prospective

NIST 800-37 Rev 2, Step 0 (Prepare)

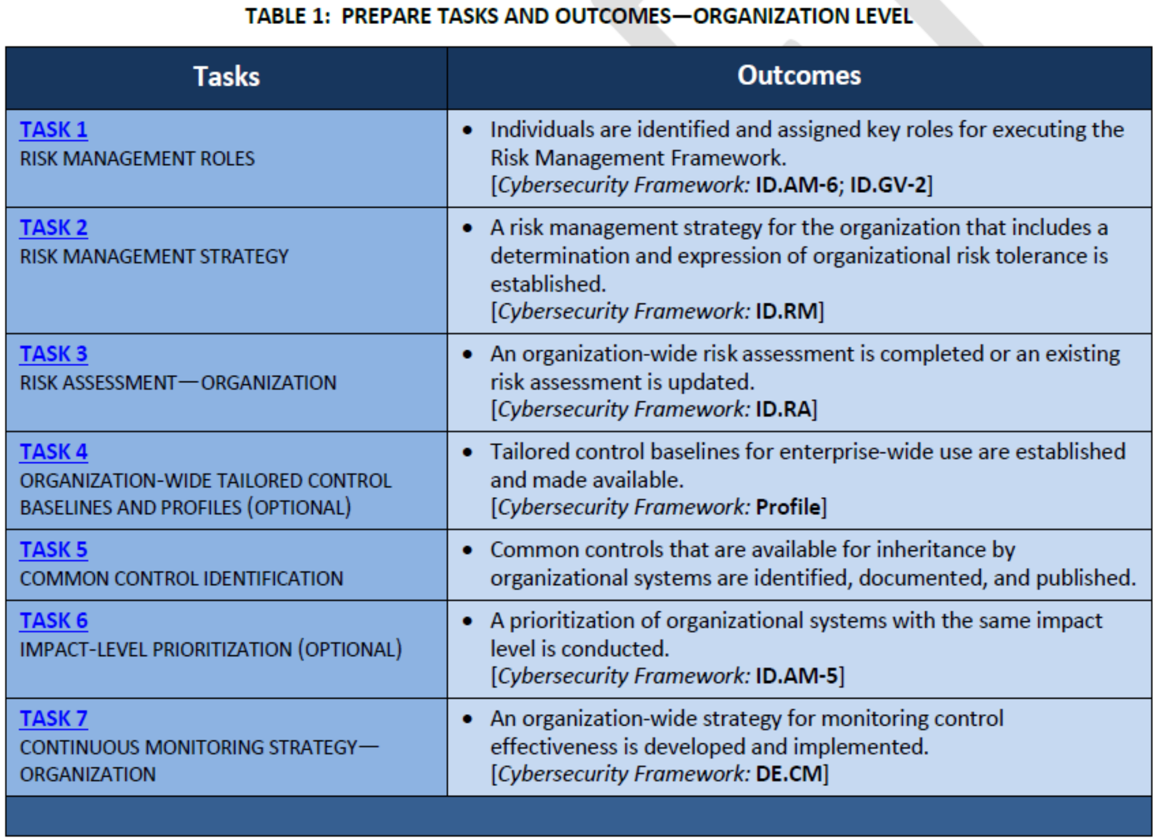


TABLE 1: PREPARE TASKS AND OUTCOMES—ORGANIZATION LEVEL

Tasks	Outcomes
TASK 1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework:* **ID.AM-6; ID.GV-2**]
TASK 2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework:* **ID.RM**]
TASK 3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework:* **ID.RA**]
TASK 4 ORGANIZATION-WIDE TAILORED CONTROL BASELINES AND PROFILES (OPTIONAL)	• Tailored control baselines for enterprise-wide use are established and made available. [*Cybersecurity Framework:* **Profile**]
TASK 5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK 6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	• A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework:* **ID.AM-5**]
TASK 7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	• An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework:* **DE.CM**]

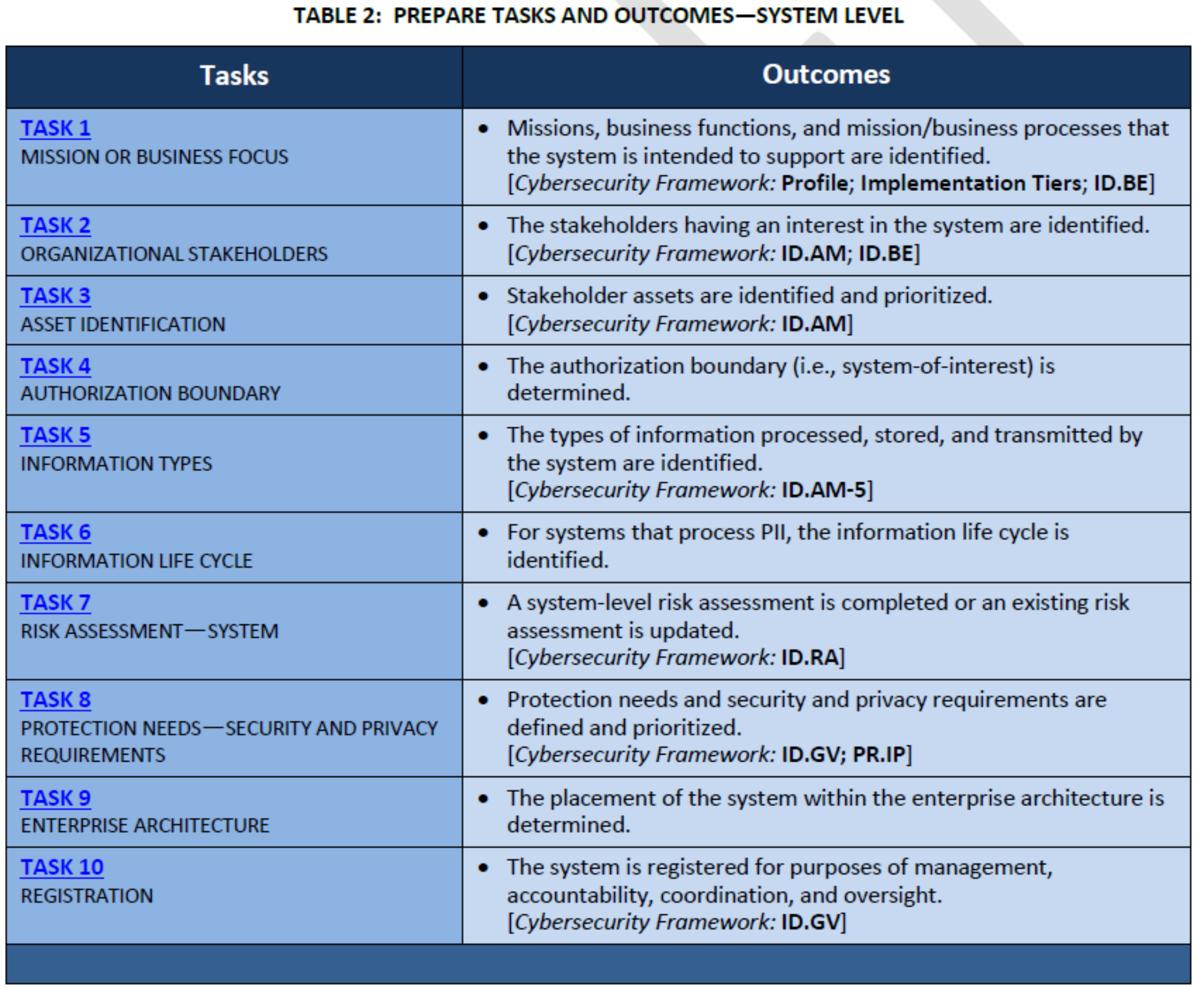
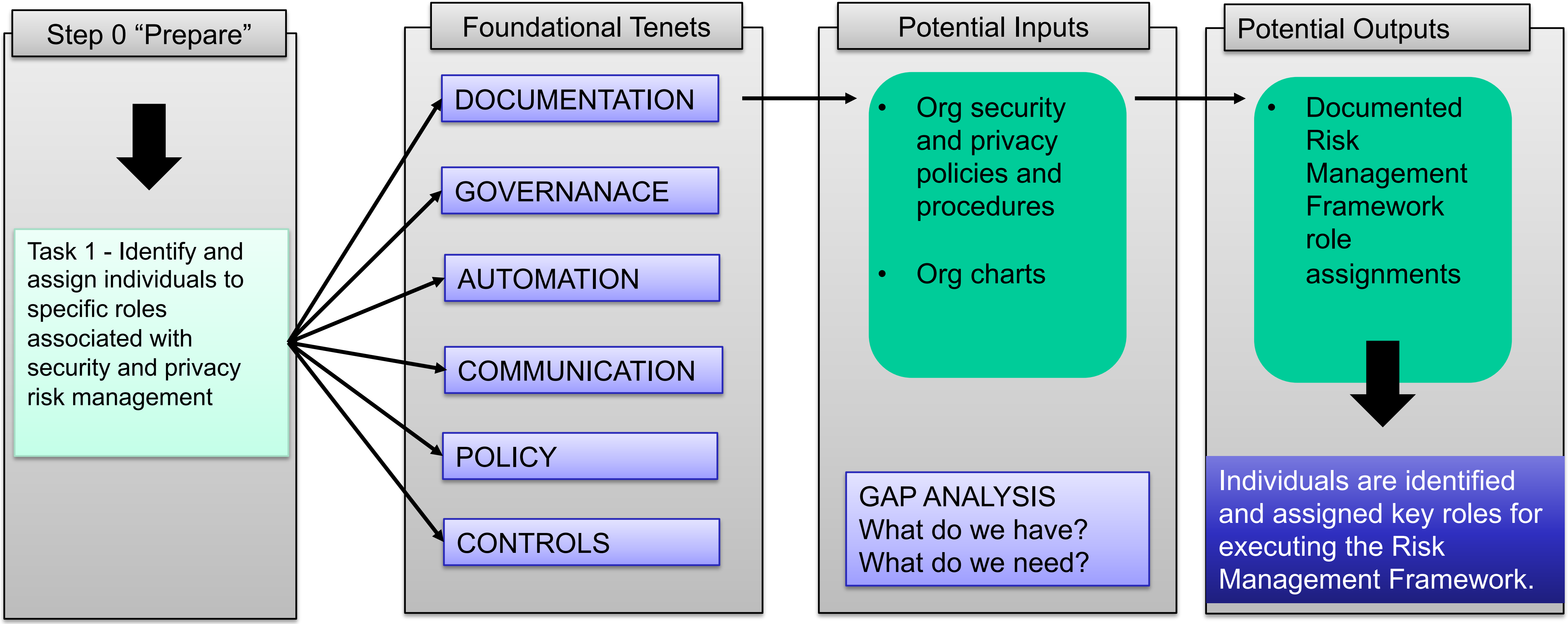


TABLE 2: PREPARE TASKS AND OUTCOMES—SYSTEM LEVEL

Tasks	Outcomes
TASK 1 MISSION OR BUSINESS FOCUS	• Missions, business functions, and mission/business processes that the system is intended to support are identified. [*Cybersecurity Framework:* **Profile; Implementation Tiers; ID.BE**]
TASK 2 ORGANIZATIONAL STAKEHOLDERS	• The stakeholders having an interest in the system are identified. [*Cybersecurity Framework:* **ID.AM; ID.BE**]
TASK 3 ASSET IDENTIFICATION	• Stakeholder assets are identified and prioritized. [*Cybersecurity Framework:* **ID.AM**]
TASK 4 AUTHORIZATION BOUNDARY	• The authorization boundary (i.e., system-of-interest) is determined.
TASK 5 INFORMATION TYPES	• The types of information processed, stored, and transmitted by the system are identified. [*Cybersecurity Framework:* **ID.AM-5**]
TASK 6 INFORMATION LIFE CYCLE	• For systems that process PII, the information life cycle is identified.
TASK 7 RISK ASSESSMENT—SYSTEM	• A system-level risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework:* **ID.RA**]
TASK 8 PROTECTION NEEDS—SECURITY AND PRIVACY REQUIREMENTS	• Protection needs and security and privacy requirements are defined and prioritized. [*Cybersecurity Framework:* **ID.GV; PR.IP**]
TASK 9 ENTERPRISE ARCHITECTURE	• The placement of the system within the enterprise architecture is determined.
TASK 10 REGISTRATION	• The system is registered for purposes of management, accountability, coordination, and oversight. [*Cybersecurity Framework:* **ID.GV**]

Tier 1 Step 0 (Prepare) - Approach



Step 0 “Prepare”

Task 1 - Identify and assign individuals to specific roles associated with security and privacy risk management

Foundational Tenets

DOCUMENTATION

GOVERNANACE

AUTOMATION

COMMUNICATION

POLICY

CONTROLS

Potential Inputs

- Org security and privacy policies and procedures
- Org charts

GAP ANALYSIS
What do we have?
What do we need?

Potential Outputs

- Documented Risk Management Framework role assignments

Individuals are identified and assigned key roles for executing the Risk Management Framework.

U.S. AIR FORCE

Tier 1 Step 0 (Prepare) - Outcomes

NIST 800-37 rev 2 RMF Steps	Tasks	Outcomes	Foundational Work Products					
			Governance	Communications	Documentation	Policy	Controls	Automation
Prepare Step 0 (Organization)	**Task 1 - Risk Management Roles**	Individuals are identified and assigned key roles for executing the Risk Management Framework.	🟩 [GV1] RMF Roles and Responsibilities Matrix	🟩 [CM1] RMF Role Based Training Plan (SCA role only)	🟩 [DO 1] RMF Role Based Training Requirements - Flowchart (SCA role only)	🟩 [PO 1] Draft AF Risk Management Strategy (annotated outline)	🟥 [CO 1] Step 0 Common Controls Matrix	🟨 [AU 1] Automation Strategy (PowerPoint)
	Task 2 - Risk Management Strategy	A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.	🟩 [GV2] List of governance bodies to execute and maintain RMF Next	🟩 [CM2] Communications Plan /Form	🟦 [DO 2] Proposed job aids for Risk Management Strategy	🟩 [PO 1] Draft AF Risk Management Strategy (annotated outline)	🟥 [CO 1] Step 0 Common Controls Matrix	🟨 [AU 1] Automation Strategy (PowerPoint)
	Task 3 - Risk Assessment - Organization	An organization-wide risk assessment is completed or an existing risk assessment is updated.	🟩 [GV3] Diagram of proposed governance structure with Risk Executive Function (REF)	🟦 N/A	🟨 [DO 3] Comments on draft Risk Assessment Strategy from A4	🟨 [PO 2] Comments on draft Risk Assessment Strategy from A4	🟥 [CO 1] Step 0 Common Controls Matrix	🟥 [AU 2] Turbo TAX ATO Proof of Concept
	Task 4 - Organization-wide Tailored Control Baselines and Profiles (Optional)	Tailored control baselines for organization-wide use are established and made available.	🟩 [GV3] Diagram of proposed governance structure with Risk Executive Function (REF)	🟦 N/A	🟨 DO 3] Comments on draft Risk Assessment Strategy from A4	🟨 [PO 2] Comments on draft Risk Assessment Strategy from A4	🟥 [CO 2] List of Organizational Tailored Control Baselines	🟨 [AU 3] ARAD Controls for System Monitoring Automation
	Task 5 - Common Control Identifitication	Common controls that are available for inheritance by organizational systems are identified, documented, and published.	🟩 [GV3] Diagram of proposed governance structure with Risk Executive Function (REF)	🟦 N/A	🟨 DO 3] Comments on draft Risk Assessment Strategy from A4	🟨 [PO 2] Comments on draft Risk Assessment Strategy from A4	🟥 [CO 3] List of Common Control Providers	🟩 [AU 4] Organizational Risk Tolerance Baseline (ORTB) Controls for Automation
	Task 6 - Impact-Level Prioritization (Optional)	A prioritization of organizational systems with the same impact level is conducted.	🟩 [GV4] Revised IT System Categorization Checklist	🟦 N/A	🟨 DO 3] Comments on draft Risk Assessment Strategy from A4	🟨 [PO 2] Comments on draft Risk Assessment Strategy from A4	🟥 [CO 1] Step 0 Common Controls Matrix	🟨 [AU 1] Automation Strategy (PowerPoint)
	Task 7 - Continuous Monitoring Strategy - Organization	An organization-wide strategy for monitoring control effectiveness is developed and implemented.	🟨 [GV5] Evaluation of DTRA continuous monitoring solution	🟨 [CM3] RMF Knowledge Service - Knowledge Management Procedures	🟥 [DO 4] Proposed updates to CM Strategy	🟥 [PO 3] proposed updates to CM Strategy	🟥 [CO 1] Step 0 Common Controls Matrix	🟥 [AU 5] Proposed automation requirements for CM

🟩 Adjudicate-Draft 🟨 Incomplete-Draft 🟦 Not Applicable 🟥 Needs Work

Next Steps

- Staff Tier 1 organizational documents
  - Cybersecurity TAG
  - HAF staffing process (as required)
- Tier 3 system level step 0 Analysis
  - *Analyze Step – 0 tasks and identify essential activities*
  - *Using the six foundational pillars*
- Develop enterprise ISCM strategy
  - IAW DOD guidance (i.e. NDAA 1653)
- Collaborate with DoD CIO Tier II reform efforts

Questions

- POC: Capt Jacob T. Mireles
- NIPR email: jacob.t.mireles2.mil@mail.mil
- Comm Phone: 703-692-6157