#### RMF used by DoD defined by

# NIST 800-37 v2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

**Preparation** is the step not listed:

**Step 1: Categorize/ Identify** – Assets, boundaries, roles and responsibilities

Step 2: Select – Security Controls to protect CIA triad

Step 3: Implement - Security Control to measure benchmarks, Policies to algin the cybersecurity frameworks

**Step 4: Assess** – Security Controls are implemented correctly

Step 5: Authorize and Step – Use reports for risk acceptance, track failed controls

6: Monitor – Continuous monitoring, automate monitoring

# 6 Steps to the NIST RMF

Administration will need to identify and categorize your organizational systems. All information types, assets and information systems need to be accounted for as well as the roles and responsibilities of those who operate it. Additionally, you will need to log intended use of each system's operation, and how each one connects to other systems.

Continuously automate your monitoring and maintain your security posture to stay in compliance and adjust to new ordinance as it is released.

Using an Integrated Risk Management solution can help automate these activities.

Use reporting to determine if permitted risks are acceptable and track failed controls. This is done with permission and oversight from staveholders and organizational representatives in an effort to keep everybody informed.

MONITOR SELECT

PREPARE

IMPLEMENT

ASSESS

Benchmark your security and privacy controls using assessment procedures to determine if controls are benign implemented correctly and producing the desired outcome.

Security controls are the specifications necessary to protect the confidentiality, integrity and availability of the organization's information security systems and critical infrastructure.

Your organization will need to enact your security controls to measure and benchmark the posture of your business. Policies should be specific and align with your cybersecurity framework initiatives.



## What is the Risk Management Framework?

- Flexible risk-based framework for managing cybersecurity risk throughout the system lifecycle
  - Used to manage Federal Gov't systems
  - · 7 defined steps
- Leverages security and privacy controls from NIST SP 800-53
- Derived from the Federal Information Security Modernization Act (FISMA)



NIST SP 800-53B - Security and Privacy Controls for Information Systems and Organizations

### Step 1 - Preparation is key

- Identify key risk management roles
  - · Senior officials with defined responsibilities
- Establish risk management strategy
  - Risk assessments
  - · Continuous monitoring
- Determine organizational risk tolerance
  - · Established thresholds





## **Step 2 - Categorize based on information types**

- Information Types inform categorization
  - NIST SP 800-60 Volumes 1 & 2 (Mapping Guidelines, Information Types w/ provisional security impact level assignments)
- Determine adverse impact on confidentiality, integrity, and availability
  - FIPS-199 System Categorization



# SCOPING OF APPROPRIATE PROTECTIONS IS DRIVEN BY DATA TYPES

FIPS PUB 199 – (FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION)
Standards for Security Categorization of Federal Information and Information Systems

FIPS PUB 200 - Minimum Security Requirements for Federal Information and Information Systems

### Step 3 - Select the appropriate security/privacy controls

- Control selection is based on risk, informed by Security Categorization
  - NIST SP 800-53 Security and Privacy Controls
  - Low, Moderate, High Baselines
- Additional considerations
  - Privacy Impact Assessment (PIA)
  - Business Impact Analysis (BIA)

# SECURITY AND PRIVACY CONTROLS SELECTED COMMENSURATE WITH IDENTIFIED RISK



NIST SP 800-53B - Security and Privacy Controls for Information Systems and Organizations

## **Step 4 - Implement the selected controls**

- Implement and operationalize security and privacy controls
- Document in a System Security Plan (SSP)
- · Supporting artifacts and processes
  - Policies/Procedures/Plans
  - CMP, ISCP, Incident Response Plan



# SECURITY AND PRIVACY CONTROLS ARE APPLIED AT THE ORG AND SYSTEM LEVEL

#### SSP - Information System Security Plan

NIST SP 800-18 Rev. 1 - Guide for Developing Security Plans for Federal Information Systems

FIPS 200 under SYSTEM SECURITY PLAN from NIST SP 800-18 Rev. 1

CNSSI 4009-2015 under system security plan (SSP) from NIST SP 800-18 Rev. 1

NIST SP 800-137 under System Security Plan from FIPS 200

NIST SP 800-30 Rev. 1 (Guide for Conducting Risk Assessments) under System Security Plan

NIST SP 800-39 (Managing Information Security Risk) under System Security Plan

NISTIR 8170 (Approaches for Fed Agencies to Use the Cybersecurity Framework) under System Security Plan

CNSSI 4009-2015 - Committee on National Security Systems (CNSS) Glossary

#### **CMP - Configuration Management Plan**

NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems

## Step 5 - Assess the control implementations

- Assess to ensure that implemented controls are meeting desired outcomes
- Security Control Assessments
  - · Interview, test, examine
- Security Assessment Report (SAR)
- and Milestones (POA&M)



#### ASSESSMENTS ENSURE THAT CONTROLS ARE APPROPRIATELY APPLIED AND OPERATING



#### **Security Control Assessment**

NIST SP 800-53A - Assessing Security and Privacy Controls in Information Systems and Organizations

#### **SAR - Security Assessment Report**

The SAR describes the risks associated with the vulnerabilities identified during [System Name]'s security assessment and also serves as the risk summary report as referenced in NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems.

POA&M - Plan of Action and Milestones

## Step 6 - Authorize the system to operate

- Senior official determines if residual security and privacy risks are acceptable
  - Reviews the authorization package (e.g., SSP, SAR, POA&M)
- System may be Authorized to Operate (ATO) by the Authorizing Official (AO)



# SYSTEM ATO IS A MAJOR MILESTONE BUT NOT THE END OF THE JOURNEY

System is documented Security controls have been implemented Tested and validated the controls are in place Senior official to authorize the system

After reviewing the SSP, SAR and POAM you make a final determination whether the system is

- ATO Authorization to Operate
- IATO Interim Authorization to Operate
- IATT Interim Authorization to Test
- DATO Denial of Authorization to Operate

### Step 7 - Monitor to ensure acceptable security posture

- After ATO, continuous monitoring ensures the security and privacy posture is maintained
- Continuous Monitoring Plan driven by a defined strategy
  - Vulnerability scanning, penetration testing, POA&M updates
- Supports ongoing authorizations

MONTIORING ENSURES THE CONTINUED ADEQUACY OF IMPLEMENTED CONTROLS



