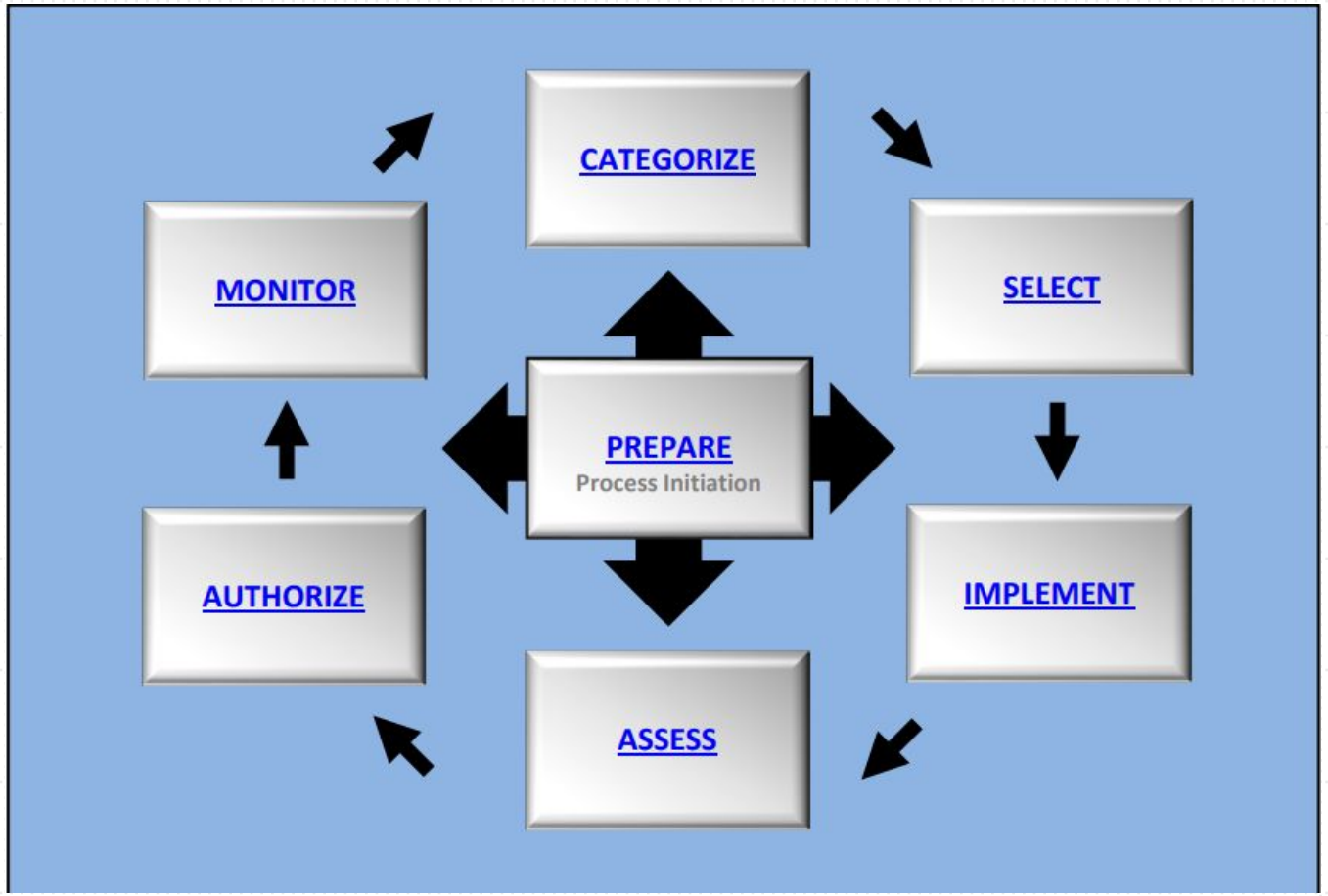
NIST Risk Management Framework (RMF)

- The RMF addresses the security concerns of organizations related to the design, development, implementation, operation, and disposal of information systems. The RMF consists of the following seven steps:



- **Prepare** to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
- **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
- **Implement** the controls and describe how the controls are employed within the system and its environment of operation.
- **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

STEP 0: Prepare

Step 0: Prepare

- Organizational Level Tasks and Outcomes

Tasks	Outcomes
TASK P-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 P-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; ID.SC**]
TASK P-3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-4 ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	• Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [*Cybersecurity Framework*: **Profile**]
TASK P-5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	• A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	• An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: **DE.CM; ID.SC-4**]

- System Level Tasks and Outcomes

Tasks	Outcomes
TASK P-8 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 P-9 SYSTEM STAKEHOLDERS	• The stakeholders having an interest in the system are identified. [*Cybersecurity Framework*: **ID.AM**; **ID.BE**]
TASK P-10 ASSET IDENTIFICATION	• Stakeholder assets are identified and prioritized. [*Cybersecurity Framework*: **ID.AM**]
TASK P-11 AUTHORIZATION BOUNDARY	• The authorization boundary (i.e., system) is determined.
TASK P-12 INFORMATION TYPES	• The types of information processed, stored, and transmitted by the system are identified. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-13 INFORMATION LIFE CYCLE	• All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system. [*Cybersecurity Framework*: **ID.AM-3**; **ID.AM-4**]
TASK P-14 RISK ASSESSMENT—SYSTEM	• A system-level risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-15 REQUIREMENTS DEFINITION	• Security and privacy requirements are defined and prioritized. [*Cybersecurity Framework*: **ID.GV; PR.IP**]
TASK P-16 ENTERPRISE ARCHITECTURE	• The placement of the system within the enterprise architecture is determined.
TASK P-17 REQUIREMENTS ALLOCATION	• Security and privacy requirements are allocated to the system and to the environment in which the system operates. [*Cybersecurity Framework*: **ID.GV**]
TASK P-18 SYSTEM REGISTRATION	• The system is registered for purposes of management, accountability, coordination, and oversight. [*Cybersecurity Framework*: **ID.GV**]

STEP 1: Categorize

Step 1: Categorization

Tasks	Outcomes
TASK C-1 SYSTEM DESCRIPTION	• The characteristics of the system are described and documented. [*Cybersecurity Framework*: **Profile**]
TASK C-2 SECURITY CATEGORIZATION	• A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [*Cybersecurity Framework*: **ID.AM-1**; **ID.AM-2**; **ID.AM-3**; **ID.AM-4**; **ID.AM-5**] • Security categorization results are documented in the security, privacy, and SCRM plans. [*Cybersecurity Framework*: **Profile**] • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. [*Cybersecurity Framework*: **Profile**] • Security categorization results reflect the organization's risk management strategy.
TASK C-3 SECURITY CATEGORIZATION REVIEW AND APPROVAL	• The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.

The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

Step 1: Categorization – The Process

Federal information systems are categorized based on the information the systems **process**, **store**, and/or **transmit**.

Information processed, stored and transmitted by a system is classified based on the impact level (Low, Moderate or High) assigned to the security objectives

- Confidentiality, Integrity and Availability (CIA)

The highest impact level – (Highest Watermark: Low, Moderate, or High) of the CIA becomes the overall categorization of the system

Systems are categorized based on the information types they store, transmit, and/or process

- Two NIST publications are used as guides in this process
  - NIST SP 800-60, Volume II, Revision I
  - FIPS 199

Step 1: Categorization – Privacy Considerations

- Privacy Threshold Assessment (PTA) and Privacy Impact Analysis (PIA)
- A Privacy Threshold Assessment (PTA) purpose is conducted to determine if the system will process, transmit or store any Personally Identifiable Information (PII).
- Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Essentially any information about you that can lead someone directly to you.
- When the system is determined to processes, transmits or stores PII, then a Privacy Impact Analysis (PIA) is conducted.
- SP 800-122

Step 1: Categorization - PII

- According to the National Institute of Standards and Technology (NIST), personally identifiable information (PII) refers to any information that can be used to distinguish or trace an individual's identity. Here are some types and examples of PII, as defined by NIST:

- 1. Identifiers:
- - Name: Full name, maiden name, alias, or initials.
- - Social Security Number (SSN): A unique identification number issued by the government.
- - Driver's license number: A unique number assigned to an individual's driver's license.
- - Passport number: A unique number assigned to an individual's passport.
- - Employee ID number: A unique number assigned to an employee by an employer.

- 2. Biometric data:
- - Fingerprints: Unique patterns of ridges and furrows on fingertips.
- - Facial recognition data: Measurements and characteristics of an individual's face.
- - Retina and iris scans: Patterns in the iris or retina of the eye.
- - DNA sequence: Genetic information unique to an individual.

Step 1: Categorization - PII

3. Financial information:
   - Credit card number: A unique number assigned to a credit card.
   - Bank account number: A unique number assigned to a bank account.
   - Tax identification number: A unique number assigned to an individual or organization for tax purposes.
   - Financial account numbers: Numbers associated with various financial accounts.

4. Contact information:
   - Address: Residential or mailing address.
   - Phone number: Personal or business phone number.
   - Email address: Personal or business email address.

5. Medical information:
   - Medical records: Information related to an individual's health or medical history.
   - Health insurance information: Policy number, coverage details, etc.
   - Prescription information: Medications prescribed to an individual.

6. Geolocation data:
   - Global Positioning System (GPS) coordinates: Geographic location coordinates.
   - IP address: A unique identifier for devices connected to a network.

Step 1: Categorization - PIA

- **Privacy Impact Analysis (PIA)** helps identify and understand any risks the system may pose to the privacy, civil rights, and civil liberties of personally identifiable information. It also elaborates on how the PII should be **handled/collected/maintained** and **protected**.
- The Privacy Impact Assessment (PIA) is a decision tool used by organizations to identify and mitigate privacy risks that notifies the public:
- What Personally Identifiable Information (PII) the organization is collecting;
- Why the PII is being collected; and
- How the PII will be collected, used, accessed, shared, safeguarded and stored.
- In most cases PTA and PIA are the responsibilities of the privacy department, however a security analyst can also be involved in this process
- Sample PIAs: DHS PIA Site

Step 1: Categorization - System of Record Notice (SORN)

- The purpose of a System of Record Notice (SORN) is to provide transparency and accountability regarding the collection, maintenance, and use of personally identifiable information by federal agencies. SORNs describe the systems of records maintained by the agencies, including the types of information collected, the individuals covered, the purposes for which the information is used, and how the information is protected.
- Sample SORN
- HHS SORNs

Step 1: Categorization – Electronic Authentication

- E-Authentication artifact is applicable when the system is accessible remotely.
- Authentication artifact involves the following:
  - Conduct a risk assessment of the information System (Risk, Vulnerability & Threats)
  - Map identified risks to the applicable assurance level (Level 1, 2, 3 or 4)
  - Select technology based on e-authentication technical guidance (Single factor, Two factor and Multi factor)
  - Validate that the implemented system has achieved the required assurance level (Test the control)
  - Periodically reassess the system to determine technology refresh requirements (Continuous assessment)

Step 1: Categorization – Electronic Authentication

Assurance Level

- Level 1: Little or no confidence in the asserted identity's validity
- Level 2: Some confidence in the asserted identity's validity
- Level 3: High confidence in the asserted identity's validity
- Level 4: Very high confidence in the asserted identity's validity

Authentication Method

- Single factor - What you know (Username password, Pin)
- Two factor - What you know and what you have (Pin and token/card)
- Multi factor what you are, where you are and what you have (Fingerprint, IP address and token)
- NIST SP 800-63

STEP 2: Select

Step 2: Select

- The purpose of the Select step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation

Tasks	Outcomes
TASK S-1 CONTROL SELECTION	• Control baselines necessary to protect the system commensurate with risk are selected. [*Cybersecurity Framework*: **Profile**]
TASK S-2 CONTROL TAILORING	• Controls are tailored producing tailored control baselines. [*Cybersecurity Framework*: **Profile**]
TASK S-3 CONTROL ALLOCATION	• Controls are designated as system-specific, hybrid, or common controls. • Controls are allocated to the specific system elements (i.e., machine, physical, or human elements). [*Cybersecurity Framework*: **Profile**; **PR.IP**]
TASK S-4 DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS	• Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents. [*Cybersecurity Framework*: **Profile**]
TASK S-5 CONTINUOUS MONITORING STRATEGY—SYSTEM	• A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [*Cybersecurity Framework*: **ID.GV**; **DE.CM**]
TASK S-6 PLAN REVIEW AND APPROVAL	• Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.

Step 2: Select – Control Baseline

- Controls are selected based on the categorization of the system. NIST SP 800-53 Rev5 provides all control baselines.
- - Low Baseline
- - Moderate Baseline
- - High Baseline

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Step 2: Select – Control Tailoring

- After selecting the control baseline, the next thing to do is to apply tailoring.
- Under Control Tailoring, 2 things are identified

1. **Identification of Control Ownership** – Common, Hybrid, and System Specific
2. **Control Applicability** – Whether the baseline controls are truly applicable to the system based on the design and operational environment of the system

Common/Inherited Controls
Refers to a security control that is implemented and shared by multiple information systems within an organization. It is a way to centralize and streamline the implementation of security measures to address common risks and requirements across multiple systems.

Examples: Policies, Technical Solutions, Physical Safeguards

Hybrid
A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control. Shared responsibility when it comes to implementation

System Specific
System team has the sole responsibility of implementing this type of control.

Step 2: Select – Relevant NIST Publications

- FIPS 200 - Minimum Security Requirements for Federal Information Systems
- NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-53B – Security Control Baselines

STEP 3: Implement

STEP 3: Implement

- The purpose of the Implement step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation.

Tasks	Outcomes
TASK I-1 CONTROL IMPLEMENTATION	• Controls specified in the security and privacy plans are implemented. [*Cybersecurity Framework*: **PR.IP-1**] • Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. [*Cybersecurity Framework*: **PR.IP-2**]
TASK I-2 UPDATE CONTROL IMPLEMENTATION INFORMATION	• Changes to the planned implementation of controls are documented. [*Cybersecurity Framework*: **PR.IP-1**] • The security and privacy plans are updated based on information obtained during the implementation of the controls. [*Cybersecurity Framework*: **Profile**]

STEP 3: Implement – Core Documents

- System Security Plan (SSP)
- Configuration Management Plan (CMP)
- Information System Contingency Plan (ISCP)
- Interconnection Security Agreements (ISAs)
- Memorandum of Understanding (MoU)
- Risk Acceptance Memos
- Waivers

STEP 4: Assess

STEP 4: Assess

- The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

Tasks	Outcomes
TASK A-1 ASSESSOR SELECTION	• An assessor or assessment team is selected to conduct the control assessments. • The appropriate level of independence is achieved for the assessor or assessment team selected.
TASK A-2 ASSESSMENT PLAN	• Documentation needed to conduct the assessments is provided to the assessor or assessment team. • Security and privacy assessment plans are developed and documented. • Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.
TASK A-3 CONTROL ASSESSMENTS	• Control assessments are conducted in accordance with the security and privacy assessment plans. • Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. • Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.
TASK A-4 ASSESSMENT REPORTS	• Security and privacy assessment reports that provide findings and recommendations are completed.
TASK A-5 REMEDIATION ACTIONS	• Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. • Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]
TASK A-6 PLAN OF ACTION AND MILESTONES	• A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [*Cybersecurity Framework*: **ID.RA-6**]

STEP 5: Authorize

STEP 5: Authorize

- The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.

Tasks	Outcomes
TASK R-1 AUTHORIZATION PACKAGE	• An authorization package is developed for submission to the authorizing official.
TASK R-2 RISK ANALYSIS AND DETERMINATION	• A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.
TASK R-3 RISK RESPONSE	• Risk responses for determined risks are provided. [*Cybersecurity Framework*: **ID.RA-6**]
TASK R-4 AUTHORIZATION DECISION	• The authorization for the system or the common controls is approved or denied.
TASK R-5 AUTHORIZATION REPORTING	• Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.