The Evolution of the RMF

May 23, 2018

Thomas G. Volpe Sr., CSSLP, PCIP

Agenda

- Background
- FISMA then and now
- RMF V1 (NIST 800-37 R1)
- Overview of the CyberSecurity Framework
- RMF V2 (NIST 800-37 R2)
- Summary

Volpe Information Technology Group, Inc.

In the beginning…

The Federal Information Security Management Act (FISMA) circa 2002

The overarching security and capital planning legislation for Federal information systems. Signed into law in 2002. **Updated in 2014.**

- Charges the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) to develop security standards and establish risk- based processes for allowing (authorizing) Federal systems to operate;
- Makes NIST standards compulsory for all agencies; FISMA eliminated an agency's ability to obtain waivers on NIST standards [Federal Information Processing Standard (FIPS)]; and
- Charges agencies to integrate information security into capital planning.

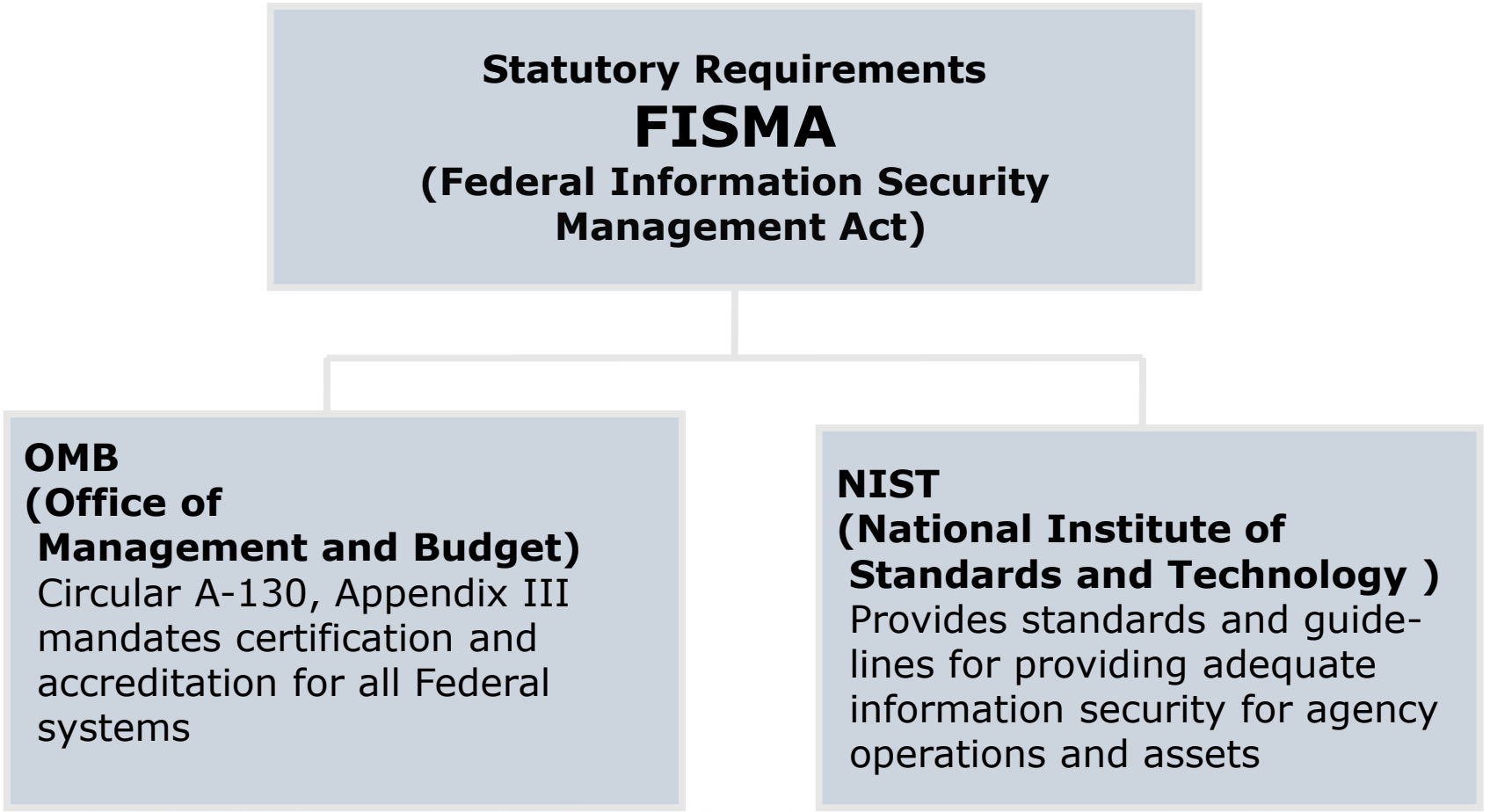
FISMA requires:

- Agency-wide information security program adoption.
- National Institute of Standards and Technology (NIST) to develop standards and guidance for Federal agencies.
- Implementation of an agency risk management program.

Volpe Information Technology Group, Inc.

In the beginning…

The Federal Information Security Management Act (FISMA)



Volpe Information Technology Group, Inc.

Modernization
The Federal Information Security ~~Management~~ Act (FISMA)

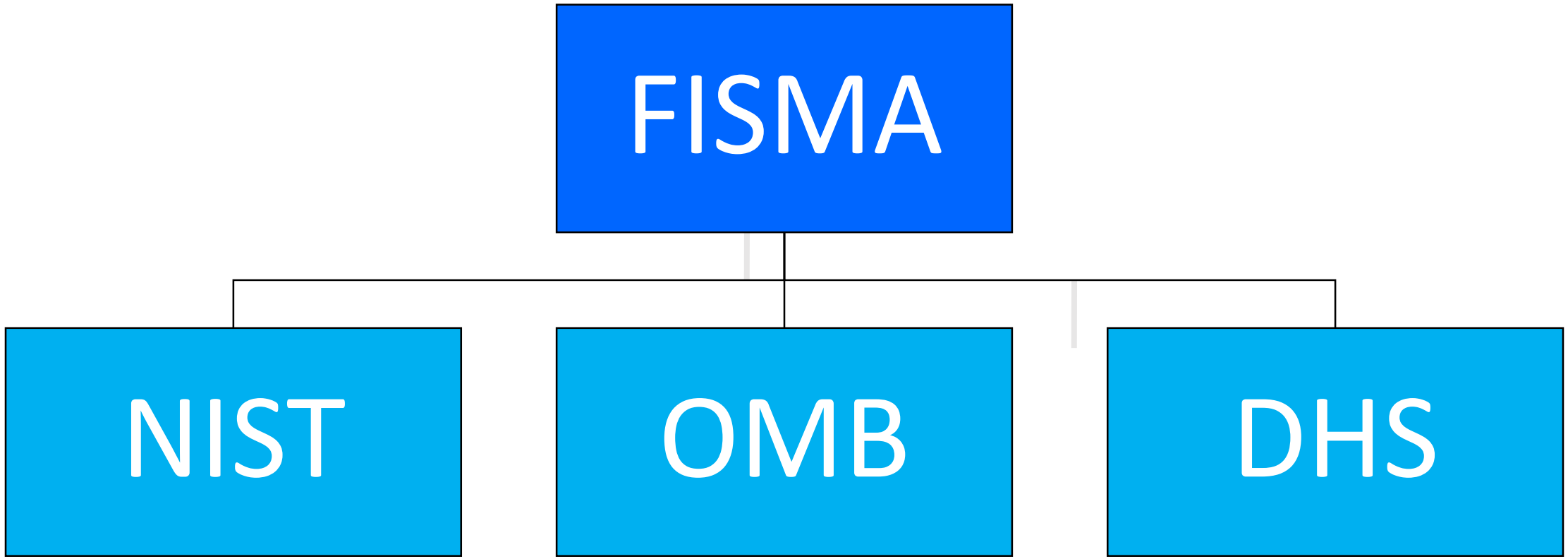
- **National Institute of Standards and Technology (NIST) to develop standards and guidelines to:**
  1. **Categorize all info and info systems**
     - **FIPS Pub. 199**
  2. **Recommend the types to be included in each category**
     - **NIST SP 800-60**
  3. **Determine minimum info security requirements**
     - **FIPS Pub. 200**
     - **NIST SP 800-53 -**

       Rev 4 is currently in use by Federal Agencies

       rev 5 DRAFT is new - Security and Privacy Controls for Information Systems and Organizations

Now…

The Federal Information Security **Modernization** Act (FISMA) (Circa 2014)



Volpe Information Technology Group, Inc.

FISMA 2002 vs. FISMA 2014

- Authorizes the Secretary of the Department of Homeland Security (DHS) to administer the implementation of information security policies and practices for information systems.
- Directs the Secretary of DHS to consult with and consider guidance developed by NIST.
- Provides for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing security procedures; and detecting, reporting, and responding to security incidents.
- Agencies to include offices of general counsel as recipients of security incident notices.
- Agencies must report to Congress any major **security incidents** within seven days after there is a reasonable basis to conclude that a major incident has occurred.
- Agencies must submit an annual report regarding major incidents to OMB, DHS, Congress and the Government Accountability Office (GAO), or Comptroller General.
- OMB required to ensure the development of guidance for evaluating the effectiveness of information security programs and practices and determining what constitutes **a major security incident**.
- Directs the Federal Information Security Incident Center (FISIC) to provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for risk assessments.
- Directs OMB to include an assessment of the agencies' adoption of continuous diagnostics technologies in their annual reports to Congress.
- Impact on contractors.

RMF 1.0 (800-37 R1)

Guide for Applying the Risk Management Framework to Federal Information Systems - A lifecycle approach (circa 2010)

The purpose of this publication is to provide guidelines for the risk-based security authorization process of Federal information systems. It was developed to enhance the security of Federal government IT systems by:

- The use of NIST SP 800-37, is required by OMB Memorandum **M-12-20**. (Guidance?)
- Integrate security into the Systems Development Lifecycle (SDLC).
- Ensuring authorizing officials are appropriately engaged throughout the risk management process;
- Promoting a better understanding of organizational risks resulting from the operation and use of information systems; and
- Supporting consistent, informed security authorization decisions. (Requirement of FISMA)

The RMF process is designed to be tightly integrated into enterprise architectures and ongoing system development life cycle processes (SDLC).

vitg
Volpe Information Technology Group, Inc.

RMF 1.0 (800-37 R1)

Guide for Applying the Risk Management Framework to Federal Information Systems - A lifecycle approach (circa 2010)

- The risk management framework changes the traditional focus of Security Assessment & Authorization (SA&A) as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions.
- It promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes.
- A cyclic process that operates around and throughout an agencies systems development lifecycle (SDLC).

RMF 1.0 (800-37 R1)

Six (6) Steps.

1. **Categorizing** info systems
   (Determine initial tailored baseline)
2. **Selecting** security controls
   (Baseline – High, Moderate, Low)
3. **Implementing** security controls
   (Configuration Management)
4. **Assessing** security controls
   (IV&V)
5. **Authorizing** info systems
   (Authority to Operate)
6. **Monitoring** security state
   (Continuous Monitoring)

vitg
Volpe Information Technology Group, Inc.

RMF 1.0 (800-37 R1)

Six (6) Steps.

Step 1: CATEGORIZE

- Security categorization is the process of determining the sensitivity of information and information systems and assigning an impact level.
- FIPS Publication 199 defines three levels (HIGH, MODERATE, LOW) of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).
- The categorization is derived from identifying the types of information stored or created within the system, and determining the expected impact to SSA from a loss in Confidentiality, Integrity, and Availability to the system or data

Step 2: SELECT CONTROLS

- The overall security categorization derived in (RMF) Step 1 is utilized to select the appropriate baseline of security controls (Low, Moderate,or High) from NIST Special Publication 800-53.
- NIST has released Revision 4 to Special Publication (SP) 800-53. This revision added additional controls to the existing security controls families as well as introduced an additional catalog of privacy controls.
- NIST SP 800-53 is separated into eighteen (18) security controls families and eight (8) privacy controls families.
- The security categorization for the system determines which controls from each family are applicable for the system.
- Certain controls and enhancements are optional and are not required for any sensitivity level. These controls are available to be used to enhance the security of the information system. An initial assessment of risk should be utilized to determine if additional security controls are necessary.

RMF 1.0 (800-37 R1)

Six (6) Steps.

Step 3: IMPLEMENT

- This step involves all activities necessary to translate the security controls identified in the System Security Plan into an effective **implementation**.
- Once the appropriate baseline and common security controls have been identified, and tailoring and supplemental guidance have been applied, the security controls must be implemented.
- NIST provides a suite of security publications to assist with the implementation of security controls (800 series).
  - Key documents include:
    - NIST SP 800-53 (Supplemental Guidance & References)
    - NIST SP 800-53A (Assessment Procedures)

Step 4: ASSESSMENT

Annual Assessment (FISMA)

- **Partial assessment**
- **Looks at a *subset* of controls**
- **Identifies and measures security compliance and the effectiveness of policies, procedures, and practices**

Security Assessment and Authorization (SA&A – formerly C&A) /Independent Verification and Validation (IV&V)

- **At least every 3 years *and upon major change***
- **Full assessment**
- **Looks at *full* set of controls**
- **Includes a risk assessment**

Volpe Information Technology Group, Inc.

RMF 1.0 (800-37 R1)

Six (6) Steps.

Step 5: AUTHORIZE

- Prepare a plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.
- Measures implemented or planned controls to correct deficiencies and to reduce or eliminate known vulnerabilities.
- The Security Assessment Report, prepared by the Security Control Assessor, provides the results of assessing the security controls in the information system (Step 4) to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements. The Security Assessment Report may also contain a list of recommended corrective actions.
- Prepare an Authorization Package (SSP, SAR, RAR, POAMs) for management (AO)
- **Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. In accepting risk, management acknowledges that it is impossible to completely eliminate risk, and at the same time asserts that it has made the best use of existing resources to address its most critical risks.**

vitg
Volpe Information Technology Group, Inc.

RMF 1.0 (800-37 R1)

Six (6) Steps.

Step 6: MONITOR

Continuous Monitoring (generic) is maintaining ongoing awareness to support organizational risk decisions.

Information security **Continuous Monitoring** is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed, analyzed and reported at a frequency sufficient to support risk-based security decisions as needed to adequately protect organization information.

The term “Continuous Diagnostics and **Monitoring**” has been replaced by the term “Continuous Diagnostics and **Mitigation**”. DHS is currently responsible for defining the requirements of the CDM program.

NIST CYBERSECURITY FRAMEWORK

- Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure.
- Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.
- Profiles help an organization to align and prioritize its cybersecurity activities with its business requirements, risk tolerances, and resources.

NIST CYBERSECURITY FRAMEWORK

Function	Question to Answer	Action
ID - Identify	What processes and assets need protection?	Develop the **organizational understanding** to manage cybersecurity risk to systems, assets, data, and capabilities.
PR – Protect	What safeguards are available?	Develop and implement the appropriate **safeguards** to ensure delivery of critical infrastructure services.
DE – Detect	What techniques can identify incidents?	Develop and implement the appropriate **activities to identify the occurrence** of a cybersecurity event.
RS – Respond	What techniques can contain impacts of incidents?	Develop and implement the appropriate **activities to take action regarding a detected cybersecurity event.**
RC - Recover	What techniques can restore capabilities?	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

RMF 2.0 (800-37 R2)

Draft NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.*

Changes originated from:

- Executive Order (E.O.) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* recognizes the increasing interconnectedness of Federal information systems and requires agency heads to ensure appropriate risk management not only for the Federal agency's enterprise, but also for the Executive Branch as a whole. The E.O. states:
  - *"…The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities..."*
  - *"…Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents…"*
- OMB Memorandum M-17-25 provides implementation guidance to Federal agencies for E.O. 13800. The memorandum states:
  - *"… An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political, and a broad range of operational risks such as information security, human capital, business continuity, and related risks…"*
  - *"… Effective management of cybersecurity risk requires that agencies align information security management processes with strategic, operational, and budgetary planning processes…"*

RMF 2.0 (800-37 R2)

Draft NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.*

Objectives for this version:

- Provide closer linkage and communication between the risk management processes and activities at the C-suite or governance level of the organization and the individuals, processes, and activities at the system and operational level of the organization;
- Institutionalize critical organization-wide risk management **preparatory activities** to facilitate a more effective, efficient, and cost-effective execution of the RMF;
- Demonstrate how the **Cybersecurity Framework can be aligned with the RMF** and implemented using established NIST risk management processes;
- Integrate privacy risk management concepts and principles into the RMF and support **the use of the consolidated security and privacy control catalog in NIST Special Publication 800-53 Revision 5**;
- Promote the development of trustworthy secure software and systems by aligning life cycle-based systems **engineering processes in NIST Special Publication 800-160** with the steps in the RMF;
- **Integrate supply chain risk management (SCRM) concepts into the RMF** to protect against untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC; and
- Provide an alternative organization-generated control selection approach to complement the traditional baseline control selection approach

RMF 2.0 (800-37 R2)

Draft NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.*

Overview of Changes:

- **Added the PREPARATION Step (0)**
  - The purpose of the ***Prepare*** step is to carry out essential activities at the organization, mission and business process, and information system levels of the enterprise to help prepare the organization to manage its security and privacy risks using the *Risk Management Framework*.
  - **Organizational Level (7 subtasks)**
    - Individuals are identified and assigned key roles for executing the Risk Management Framework.
    - A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.
    - An organization-wide risk assessment is completed or an existing risk assessment is updated.
    - Tailored control baselines for organization-wide use are established and made available
    - Common controls that are available for inheritance by organizational systems are identified, documented, and published.
    - A prioritization of organizational systems with the same impact level is conducted.
    - An organization-wide strategy for monitoring control effectiveness is developed and implemented

RMF 2.0 (800-37 R2)

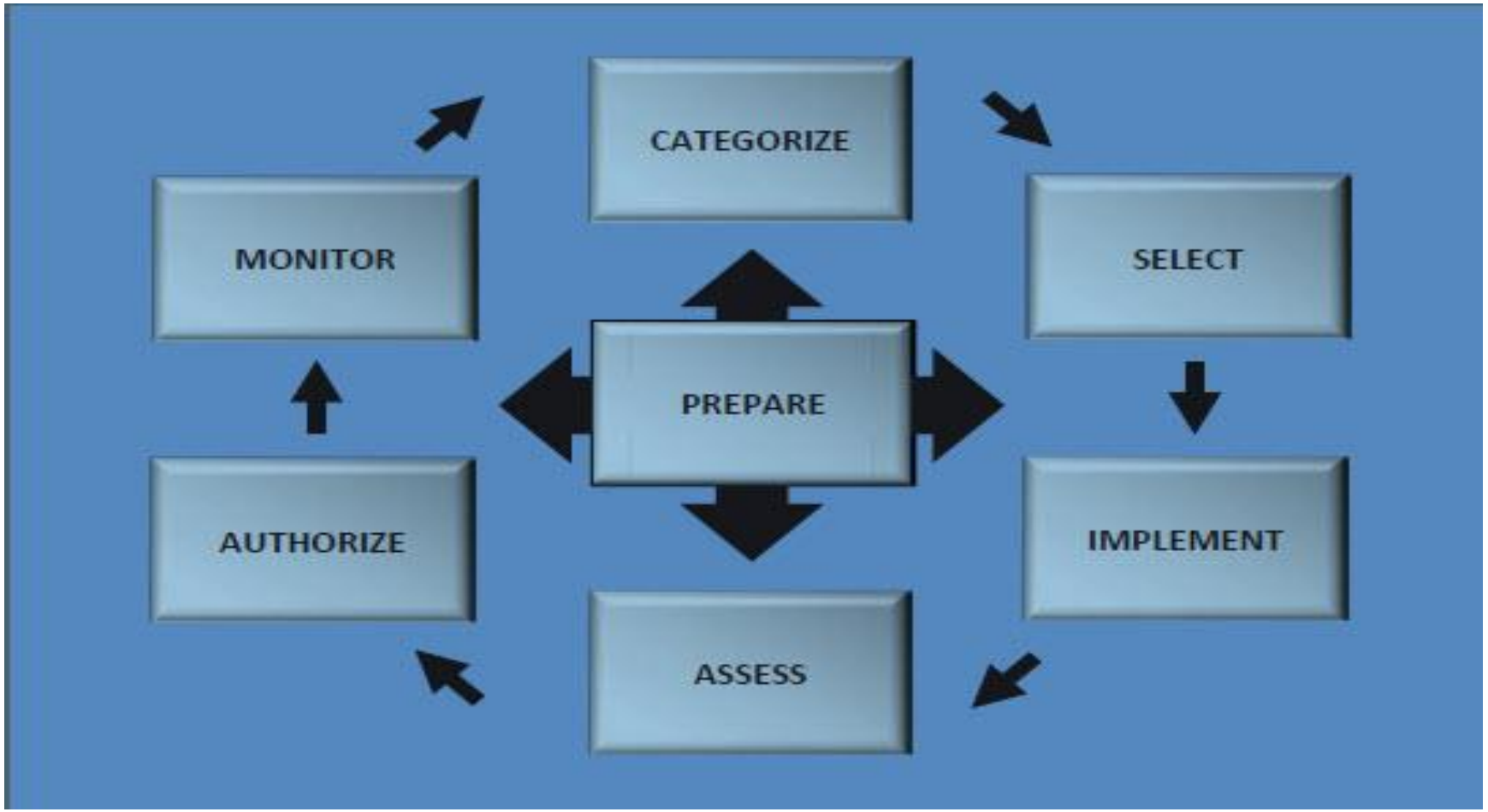
Draft NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.*

Overview of Changes (cont.):

- **Addition of PREPARATION Step (0)**
  - **System Level (10 subtasks)**
    - Missions, business functions, and mission/business processes that the system is intended to support are identified.
    - The stakeholders having an interest in the system are identified.
    - Stakeholder assets are identified and prioritized.
    - The authorization boundary (i.e., system-of-interest) is determined.
    - The types of information processed, stored, and transmitted by the system are identified.
    - For systems that process PII, the information life cycle is identified.
    - A system-level risk assessment is completed or an existing risk assessment is updated
    - Protection needs and security and privacy requirements are defined and prioritized.
    - The placement of the system within the enterprise architecture is determined
    - The system is registered for purposes of management, accountability, coordination, and oversight

RMF 2.0 (800-37 R2)

Draft NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.*



Volpe Information Technology Group, Inc.

SUMMARY DISCUSSION

- The current landscape: *It's a dangerous world in cyber space!!!*
  - *Equifax, OPM Breach, the list goes on…*
- Risks continue (threats, vulnerabilities, likelihoods, impacts) to organizations and governments.
- Everything in technology grows ever more complex.
- Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.
- Our data (both sensitive and not) is everywhere.
- Protecting critical systems and aspects is the highest priority for the US.

SUMMARY DISCUSSION (Cont)

- Federal Government Modernization Strategy
  - Identify and develop federal shared services.
  - Move to FedRAMP-approved cloud services.
  - Isolate and strengthen protection for high value assets.

Reduce and manage the complexity of systems and networks…

Engineering more trustworthy, secure, and resilient solutions.

In 3 words..

SIMPLIFY, INNOVATE and AUTOMATE

Volpe Information Technology Group, Inc.

Contact Us

3918 Vero Rd, Suite C

Baltimore, MD 21227

www.volpegroup.com

info@volpegroup.com

(410) 371-4960

Volpe Information Technology Group, Inc.