The NIST Risk Management Framework

About me…

Joe Klein, CISSP…

Computer Scientist, MITRE

Fellow, IPv6 Forum

International Speaker

Inventor - Soon to be Author

Auditor – Assessor– Pen Tester – Red Team

Chief Security Officer – IDS/Firewall geek - OSINT

Dad and Granddad - Defcon Goon

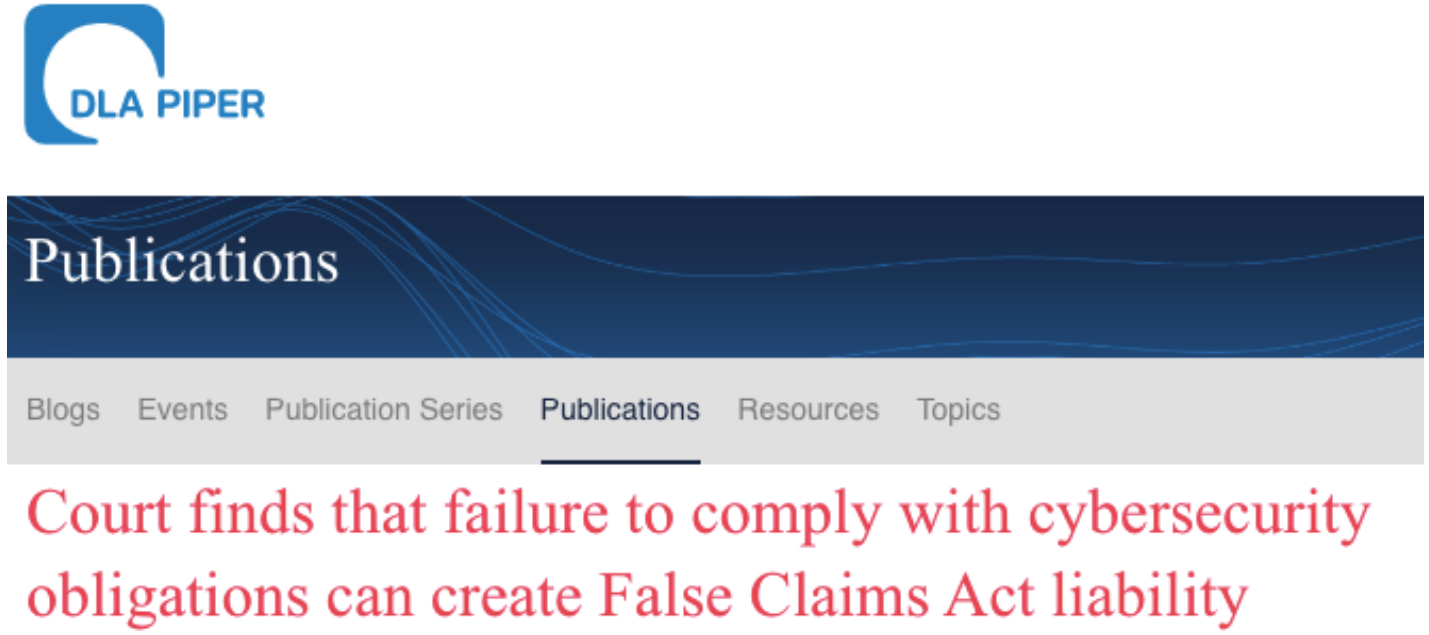
jsklein@gmail.com @JoeKlein KD4HAX

Legal Disclosure

The author's affiliation with MITRE is provided for identification purposes only, and is not intended to convey or imply MITRE’s concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.

RISK Management – After the Fact

Why Risk Management is Important



Government contractor can be sued under the False Claims Act when it misrepresents its compliance with cybersecurity-related contractual obligations, in this case SP 800-171 controls as required under the FAR/DFARS.

Reference: https://www.dlapiper.com/en/us/insights/publications/2019/05/court-finds-that-failure-to-comply-with-cybersecurity-obligations/

Learning Objectives

- Part 1: Background of the Risk Management Framework, including the federal laws and documents driving it
- Part 2: The updates to the RMF, incorporated in version 2.0 (SP 800-37 r2)
- Part 3: Core terms and definitions used by the RMF
- Part 4: How the Risk Management Framework can be used on a system (limited to the first three steps, not all seven due to time)

Part I: Background of the Risk Management Framework, the origins and driving forces

Part I: The Background
Section 1: The Law

FISMA – The Federal Law

FISMA History – OMB A-130

- First issued in December 1985
- Designed to meet information resource management requirements that were included in the Paperwork Reduction Act (PRA) of 1980.
- Specifically, the PRA assigned responsibility to the OMB Director to…
  - *develop and maintain a comprehensive set of information resources management policies for use across the Federal government, and to promote the application of information technology to improve the use and dissemination of information in the operation of Federal programs*
- In other words, Circular A-130 can be thought of as a "one-stop shopping document for OMB policy and guidance on information technology management"

NIST Introduction Into FISMA

- The National Institute of Science and Technology (NIST) tasked to address the FISMA information security standards and guidelines
- NIST standards and guidelines only apply to national security systems with express approval of appropriate federal officials for those systems
- NIST standards and guidelines are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Federal Information Security *Management* Act

- Created in 2002
- Designed to address the importance of information security to the economic and national security interests
- To require federal agencies to develop, document, and implement an agency-wide information security program
- To implement a risk-based approach / policy for cost-effective security

FYI: Fine Print

Federal Information Security ***Management*** Act (FISMA) 2002

Federal Information Security ***Modernization*** Act (FISMA) 2014:

Part I: The Background
Section 2: Who is NIST?

Who is NIST?

- The National Institute of Standards and Technology
- A part of the Department of Commerce
- Located in Gaithersburg Maryland

What Are the NIST 800 series Publications?

- Publications in NIST's Special Publication (SP) 800 series present information of interest to the computer security community.
- The series comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities.
- SP 800 publications are developed to address and support the security and privacy needs of U.S. Federal Government information and information systems.
- NIST develops SP 800-series publications in accordance with its statutory responsibilities under the Federal Information Security Modernization Act

Examples of NIST 800 Series Guidance Documents

- 800-66 Resource Guide for Implementing the HIPAA Security Rule
- 800-12 Introduction to Information Security
- 800-30 Guide for Conducting Risk Assessments
- 800-115 Technical Guide to Information Security Testing and Assessment,
- 800-171 Protecting Controlled Unclassified Information

Examples of NIST 800 Series (cont)

- 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information
- 800-124 Guidelines for Managing the Security of Mobile Devices
- 800-111 Guide to Storage Encryption Technologies for End User Devices
- 800-146 Cloud Computing Synopsis and Recommendations

Some of the Key NIST Documents for RMF

Federal Information Processing Standard **(FIPS) 199**, "Standards for Security Categorization of Federal Information and Information Systems."

Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems."

NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."……The RMF process

NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations."

Who is the Godfather of all of this?

Dr. Ron Ross

Part I: The Background

Section 3: The Introduction of the Risk Management Framework

In Layman's Terms.. the RMF….

- The Risk Management Framework (RMF) is a set of criteria that dictate how United States government IT systems must be architected, secured, and monitored.

RMF History: RMF Development and Future

- Risk Management Framework (first documented in NIST Special Publication 800-37) was developed by NIST in 2010 as a key element of the FISMA Implementation. Intended to:
  - Bring together all of the FISMA-related security standards and
  - Provide guidance and promote comprehensive and balanced information security programs by agencies

The Original Objectives of the NIST RMF

- Improve information security
- Strengthen risk management processes
- Encourage reciprocity among federal agencies
- Achieve compliance with policy directives such as the FISMA and OMB Circular A-130

Quick Overview of the Original NIST RMF Process – The Steps

1. **C**ategorize the information system and the information processed Select security controls
2. **S**elect an initial set of baseline security controls
3. **I**mplement the security controls
4. **A**ssess the security controls
5. **A**uthorize the information system operation based on residual risk
6. **M**onitor the security controls effectiveness

*** Version 2.0 as added a "Prepare Step"*

Part I: The Background

Section 4: The Recent Changes in Federal Law and the Associated Updates to the Risk Management Framework

FISMA 2014 Update

The Federal Information Security Modernization Act (FISMA) 2014: Amends FISMA 2002 with less reporting, strengthened monitoring, and focus on the issues caused by security incidents.

Included the update to the core document, Circular A-130, which was amended to:

- Eliminate inefficient and wasteful reporting
- Emphasize roles in the Federal information lifecycle
- Shift requirements from compliance exercises to crucial continuous risk-based program

Executive Order (E.O.) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

- Recognizes the increasing interconnectedness of Federal information systems
- Requires heads of agencies to ensure appropriate risk management including activities to
  - *protect IT and data from unauthorized access and other cyber threats,*
  - *maintain awareness of cyber threats,*
  - *detect anomalies and incidents adversely affecting IT and data, and*
  - *mitigate the impact of, respond to, and recover from incidents*

OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

- *"… 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…"*

OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

- Mandates that Federal agencies report their security risk management assessments to Department of Homeland Security (DHS)
- Agencies plans to implement security frameworks
- Agencies updates to the implementation
- Agencies must implement the NIST Cybersecurity Framework (CSF)

OMB Circular A-130, *Managing Information as a Strategic Resource*

- Requires agencies to implement the RMF that is described in this guideline and requires agencies to integrate privacy into the RMF process.
- Emphasizes the need for both programs to collaborate on shared objectives

Part I: The Background

Section 5: Changes to the NIST RMF

RMF Version 1 vs Version 2 – The Titles

- **Version 1 title:**

Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

- **Version 2 title:**

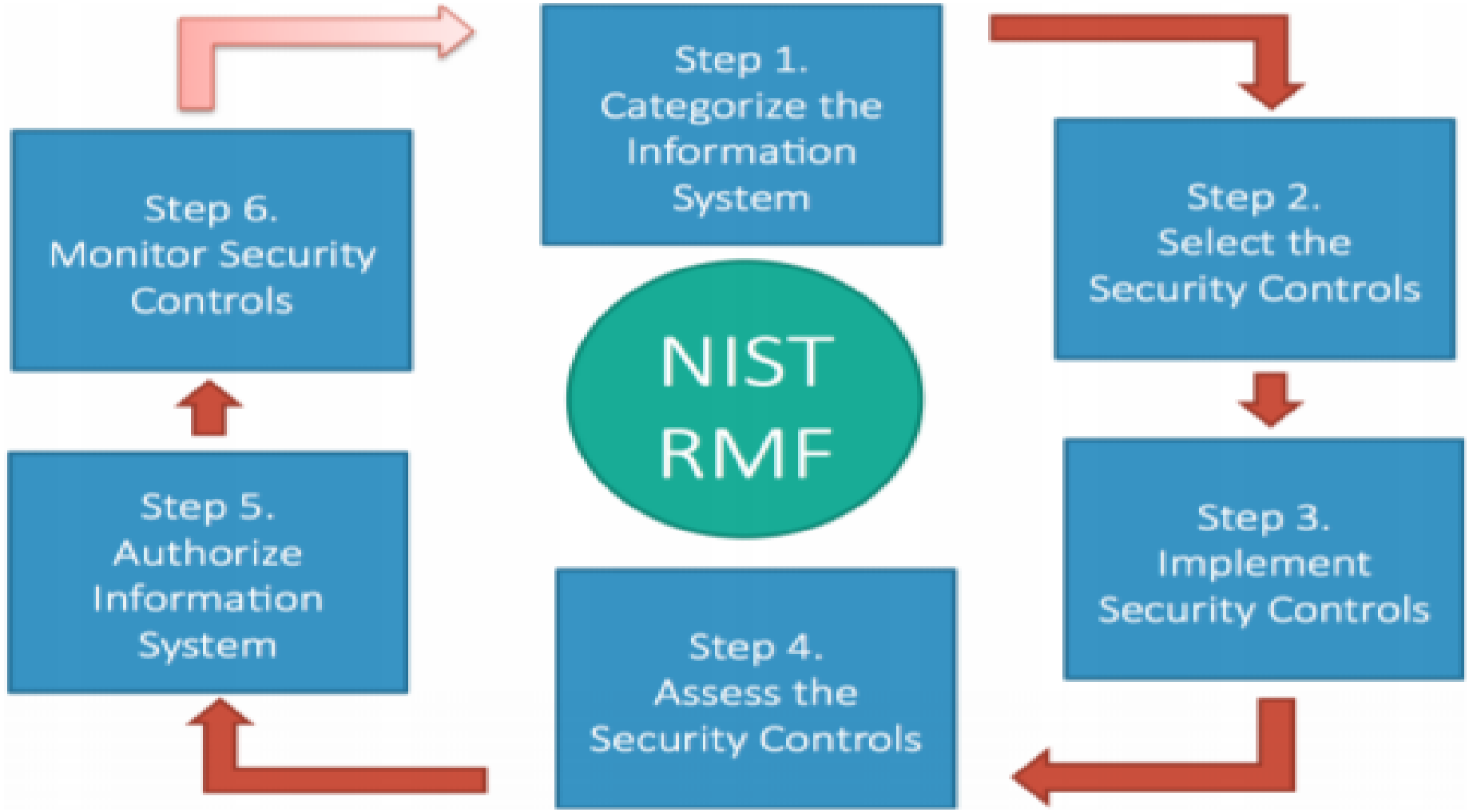
Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

RMF Focus Changes

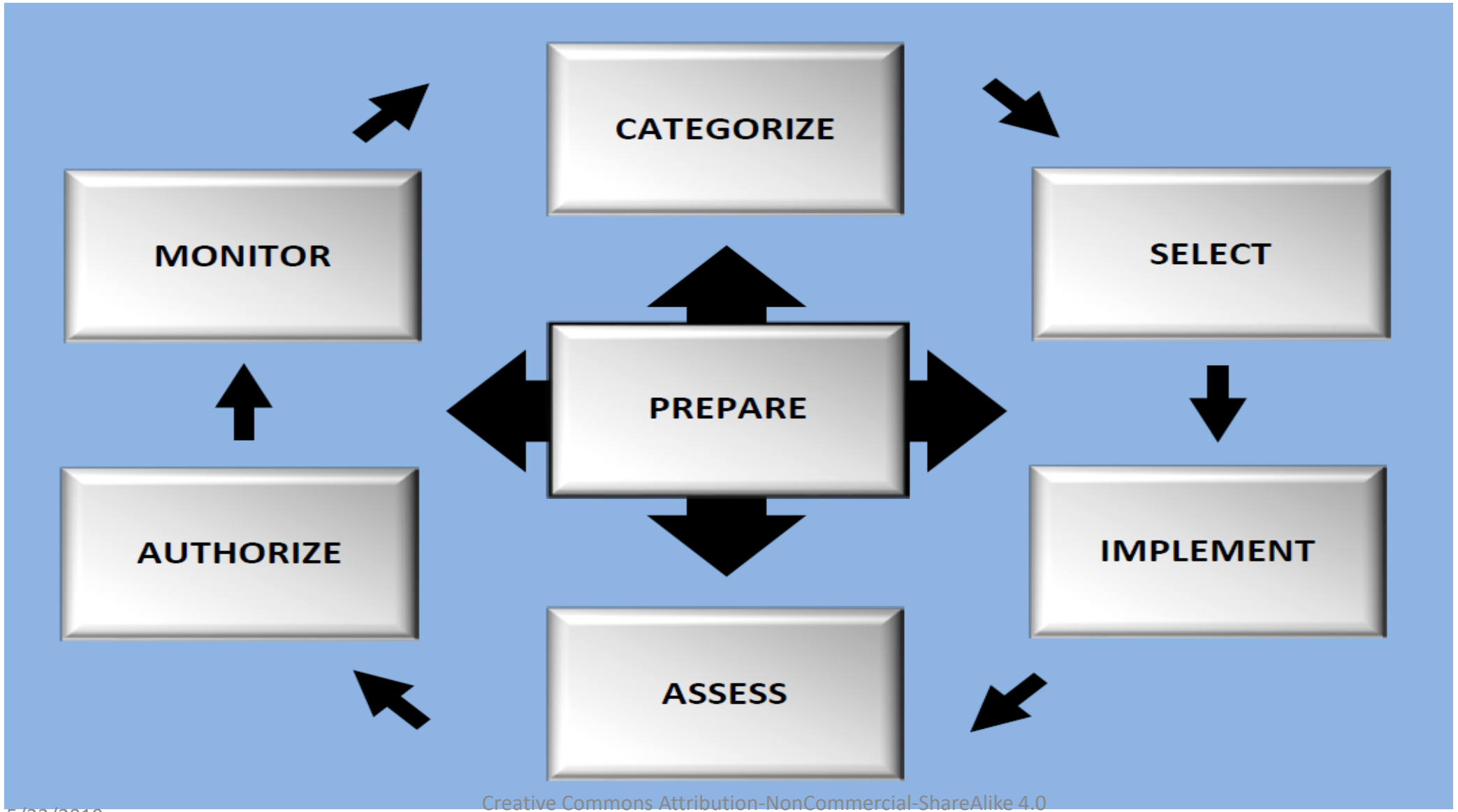
- **Version 1:** Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- **Version 2:** Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

- *Shift away from focusing on Federal Information Systems (commercial use)*
- *Heavier focus on the concept of privacy*
- *Alignment with the Cybersecurity Framework (CSF), including the renaming of previous steps or tasks to align with those in the CSF*
- *A focus shift to ensure the focus is on a process and not a checklist*
- *New focus on innovation and automation*
- *Alignment with the updates to the control set (SP 800-53 r5)*

RMF Version 1 / NIST SP800-37r1



RMF Version 2 / NIST SP800-37r2



The Seven Objectives of the RMF 2.0 Update

- To 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;
- To institutionalize critical risk management preparatory activities at all risk management levels to facilitate a more effective, efficient, and cost-effective execution of the RMF;
- To demonstrate how the NIST Cybersecurity Framework [NIST CSF] can be aligned with the RMF and implemented using established NIST risk management processes;

The Seven Objectives (cont)

- To integrate privacy risk management processes into the RMF to better support the privacy protection needs for which privacy programs are responsible;
- To promote the development of trustworthy secure software and systems by aligning life cycle-based systems engineering processes in NIST Special Publication 800-160, Volume 1 [SP 800-160 v1], with the relevant tasks in the RMF;

The Seven Objectives (cont)

- To integrate security-related, supply chain risk management (SCRM) concepts into the RMF to address untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC; and
- To allow for an organization-generated control selection approach to complement the traditional baseline control selection approach and support the use of the consolidated control catalog in NIST Special Publication 800-53, Revision 5.

The Updated RMF Process

1. *new* “**Prepare**”

   Per NIST, the prepare phase: *carries 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.*

2. Categorize the information system and the information processed Select security controls
3. Select an initial set of baseline security controls
4. Implement the security controls
5. Assess the security controls
6. Authorize the information system operation based on residual risk
7. Monitor the security controls effectiveness

The new “Prepare” Step

- To facilitate effective communication between senior leaders and executives at the organization and mission/business process levels and system owners at the operational level;
- To facilitate organization-wide identification of common controls and the development of organizationally-tailored control baselines, reducing the workload on individual system owners and the cost of system development and asset protection;
- To reduce the complexity of the information technology (IT) and operations technology (OT) infrastructure using Enterprise Architecture concepts and models to consolidate, optimize, and standardize organizational systems, applications, and services;

The new “Prepare” Step (con’t)

- To reduce the complexity of systems by eliminating unnecessary functions and security and privacy capabilities that do not address security and privacy risk; and
- To identify, prioritize, and focus resources on the organization’s high value assets (HVA) that require increased levels of protection—taking measures commensurate with the risk to such assets.

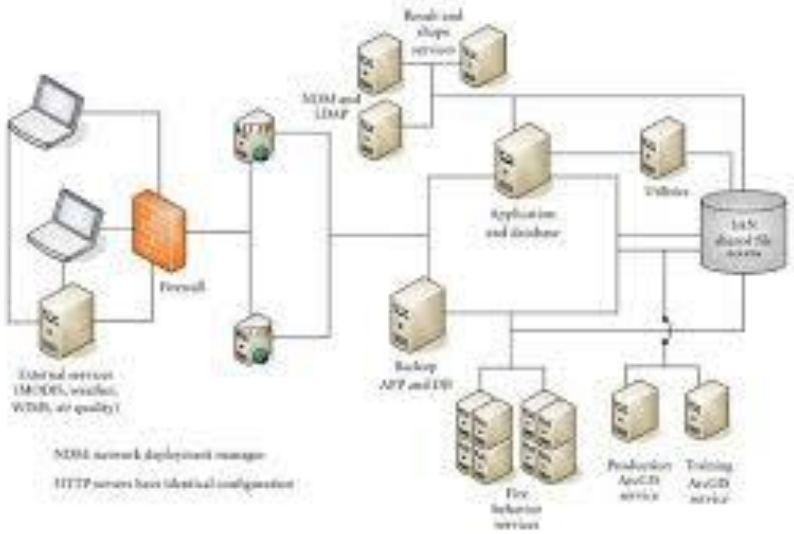
Part III: Risk Management Core
Section 1: Basic Terms

System

- Should a risk assessment be focused only on where the data resides, such as a database?
- Should it include devices with the ability to access the system such as a terminal or computer?
- Should it include mechanisms for displaying the data such as websites?
- Should it include the underlying infrastructure such as Vmware, networkers, backup storage units?

System

- **Definition of a System**: An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.



Assessment and Authorization (A&A)

- Someone needs to “vouch” for the system that it is secure
- To have someone vouch for the system, a validation process must be completed
- In the Federal Government, the validation process is call the “A&A”, Assessment and Authorization
- This was formerly called “C&A”, Certification and Accreditation

Authority to Operate (“ATO”)

- The person who vouches for the system is responsible for giving the “Authority to Operate” (ATO) designation that the system is secure enough to conduct business

Authorizing Official ("AO")

- The person who vouches for the system
- A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

System Security Plan (“SSP”)

- Provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
- A roadmap of how the system will be secured
- Contains technical specifics of the system

+

+

Security and Privacy Control

- A security control or privacy control that is implemented in an information system in part as a common control and in part as a system-specific control.
- A situation in which an information system or application receives protection from **security controls**(or portions of **security controls**) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to .

Security Control

- A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

System-Specific Control

- A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

Common Control

- Common controls are security controls that can support multiple information systems efficiently and effectively as a common capability.
- A security control that is inheritable by one or more organizational information systems
- They typically define the foundation of a system security plan
- They are the security controls you inherit as opposed to the security controls you select and build yourself
- Think of shared services and devices such as Firewall, Scanning, Back up Capabilities, and Physical and Environmental Controls

Security Control Inheritance ("Inheritance")

- A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

Hybrid Security Control

- A security control that is implemented in an information system in part as a common control and in part as a system-specific control.

Federal Enterprise Architecture

- A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

Security Control Assessment (“SCA”)

- The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

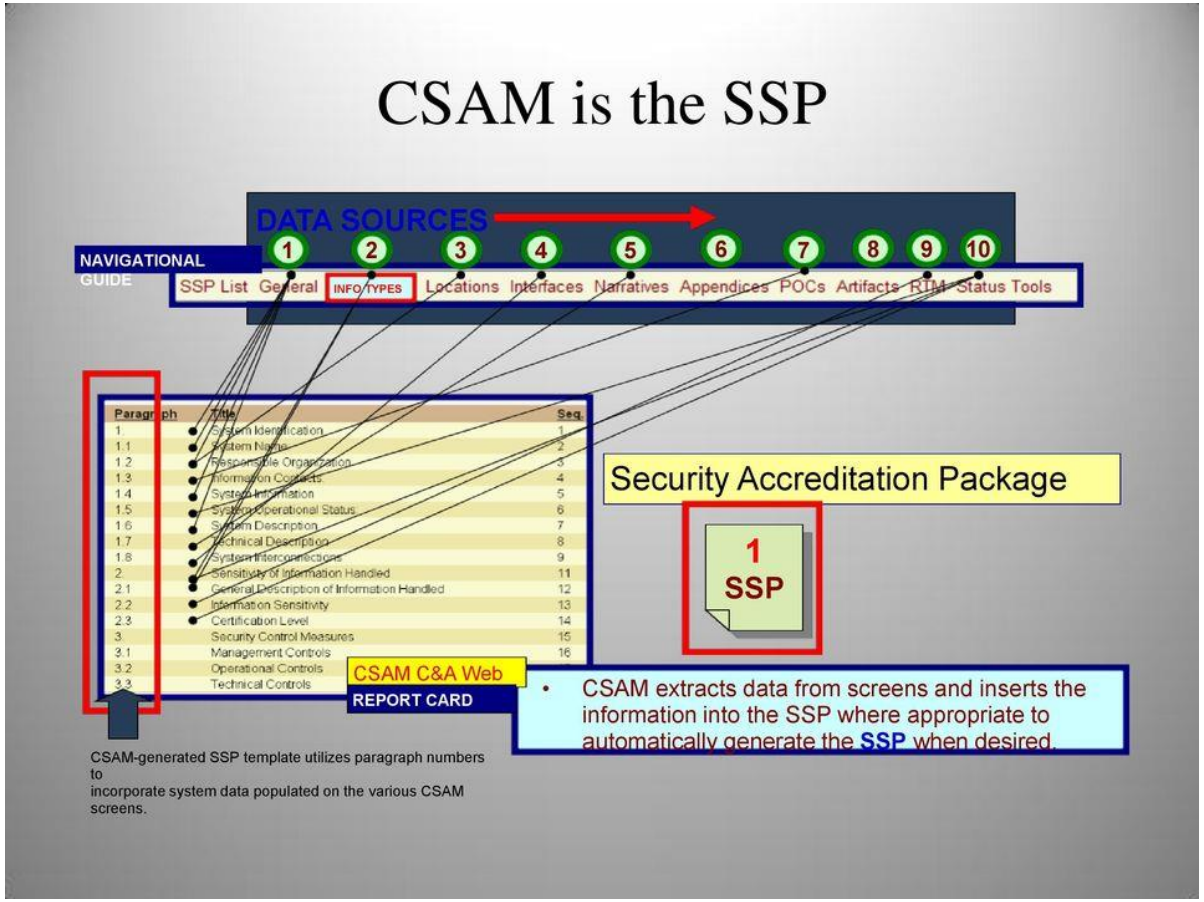
Plan of Action and Milestone (“POAM”)

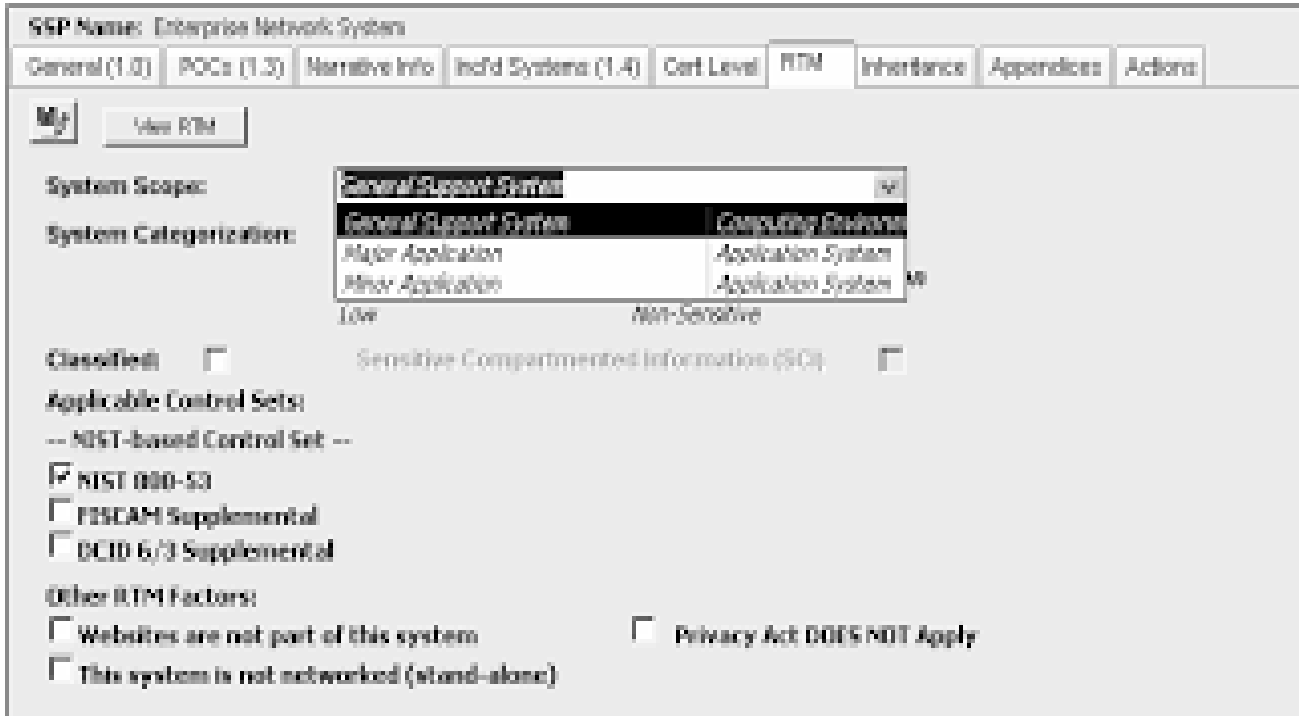
- A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Privacy Impact Assessment (“PIA”)

- An analysis of how information is handled:
  - (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
  - (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and
  - (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks

Cyber Security Assessment & Management (“CSAM”)





Cyber Security Evaluation Tool (“CSET”)

Part II: Risk Management Core
Section 2: The Big Picture

The Two Main Activity Cycles

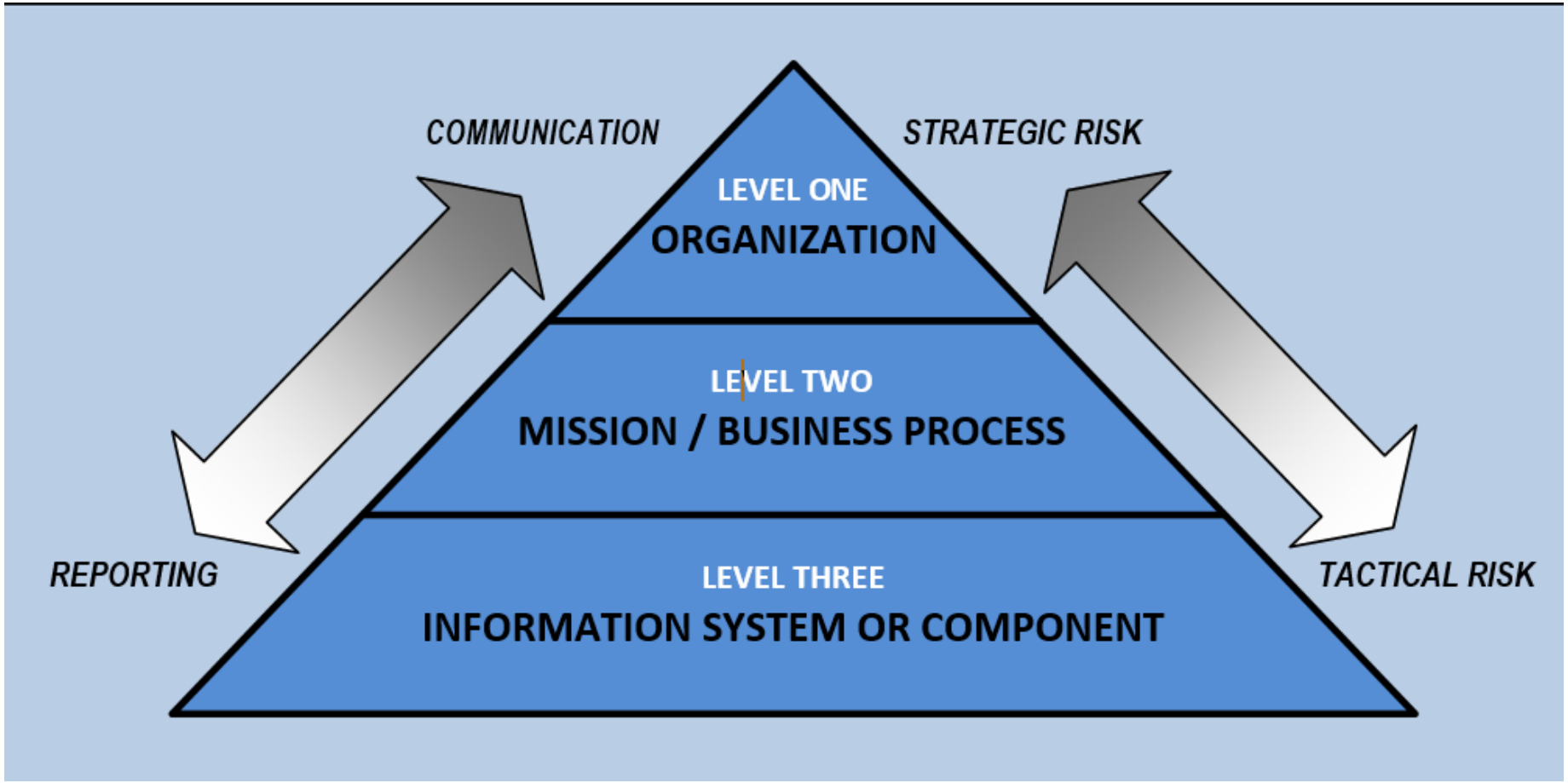
Part 1 – The creation of the System Security Plan (the SSP)

- A roadmap of how the system will be secured
- Contains technical specifics of the system
- Details the security controls provided by NIST and how they are implemented by the system, if appropriate

Part 2 - The Security Assessment of the SSP

- The testing of the System Security Plan (SSP) to ensure the intended security controls are implemented to achieve adequate security

Risk from the Top Down



Risk Layers

- Level 1 (organization) and 2 (mission/business) activities that prepare the organization for the execution of the RMF, Level 3 (technical) addresses risk from an *information system* perspective and is guided and informed by the risk decisions at the organization and mission/business process levels.
- The risk decisions at Levels 1 and 2 impact the selection and implementation of controls at the system level.
- System security and privacy requirements are satisfied by the selection and implementation of controls from NIST Special Publication 800-53 (also known as the technical bible.

Privacy Control vs Security Control

- A *privacy control* is defined as an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements and to manage privacy risks.
- A *security control* is defined as a safeguard or countermeasure prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

Part IV: How the Risk Management Framework is Implemented

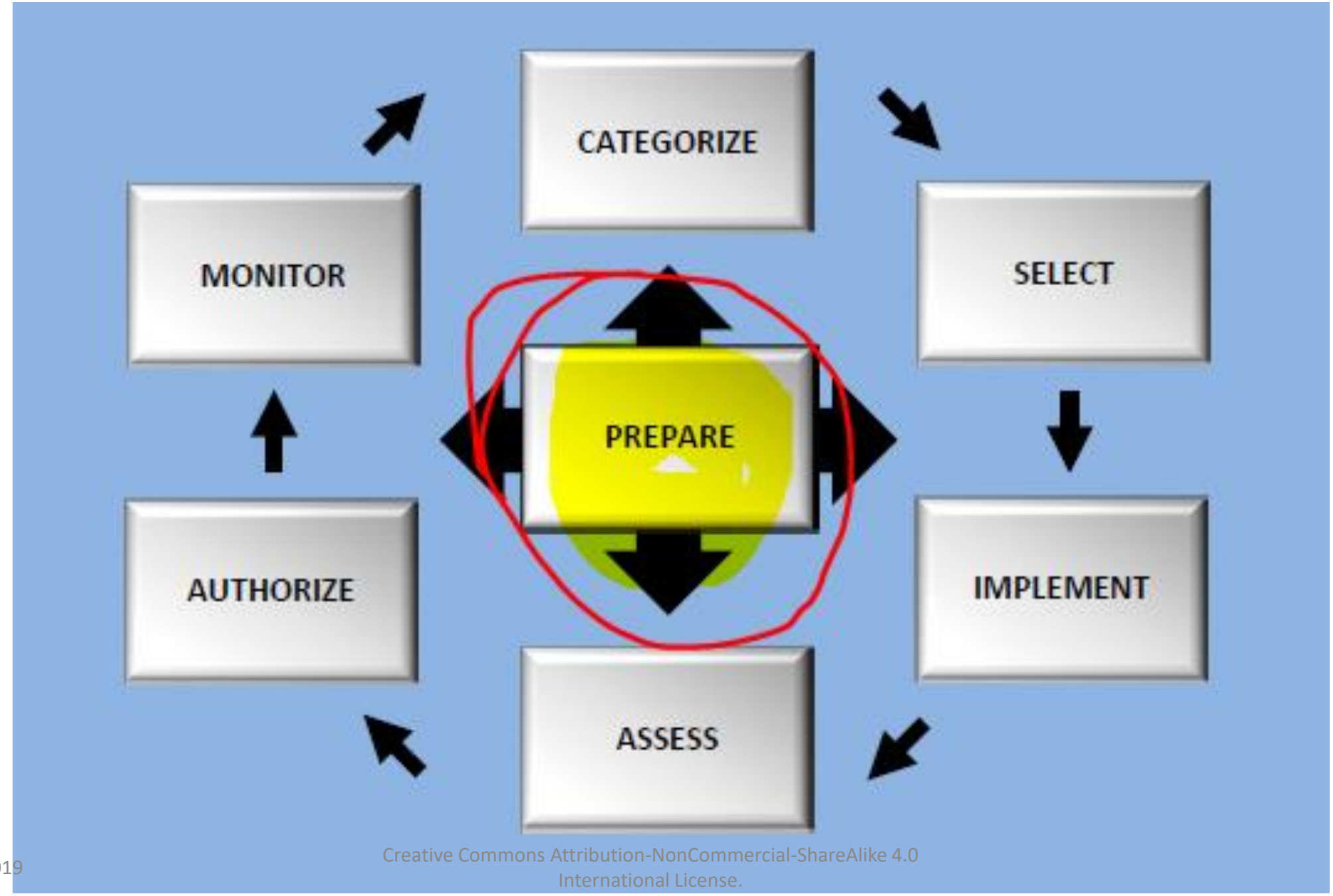
Part IV: How the Risk Management Framework is Implemented

NOTE: *This presentation will only cover the first three steps*

1) Prepare
2) Categorize
3) Select

Due to time constraints. The remaining steps will be covered in another presentation

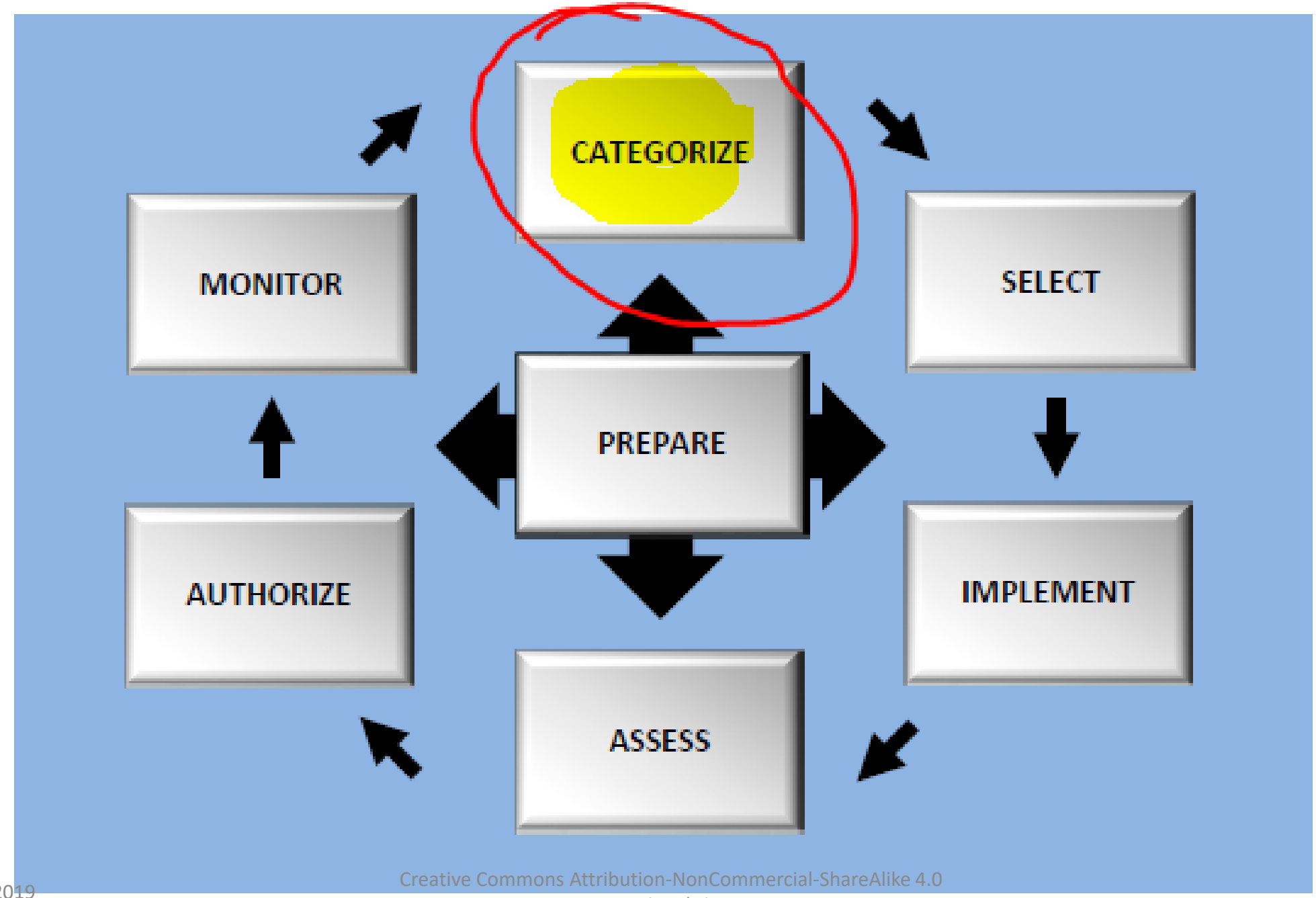
Part IV: How the Risk Management Framework is Implemented
Part 1: The Actual Steps
Subpart A: *Prepare Step*



Prepare Step

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 organization-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**]

Part II: Risk Management Core
Part 3: The Actual Steps
Subpart B: *Categorize Step*



Categorize Task 1 – Security Categorization

- A security categorization of the system, including the information processed by the system represented by the organization- identified information types, is completed.
- Security categorization results are documented in the system security and supply chain risk management plans.
- Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes.
- Security categorization results reflect the organization's risk management strategy.

Task 2 – Security Categorization Review and Approval

- The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.

Categorize Task 3 – System Description

- The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.

Categorization Foundations

- Heavily based on the CIA triad
  - Confidentiality
  - Integrity
  - Availability
- Use the CIA to categorize the system based on two areas
  - Information systems
  - Information types
- Guidance comes from several sources
  - FIPS 199
  - FIPS 200

Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of confidentiality is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"	A loss of integrity is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…"	A loss of availability is the disruption of access to or use of information or an information system.

Types and Systems

- Information Types
  - The actual data
- Information Systems
  - The hardware and software associated with the data

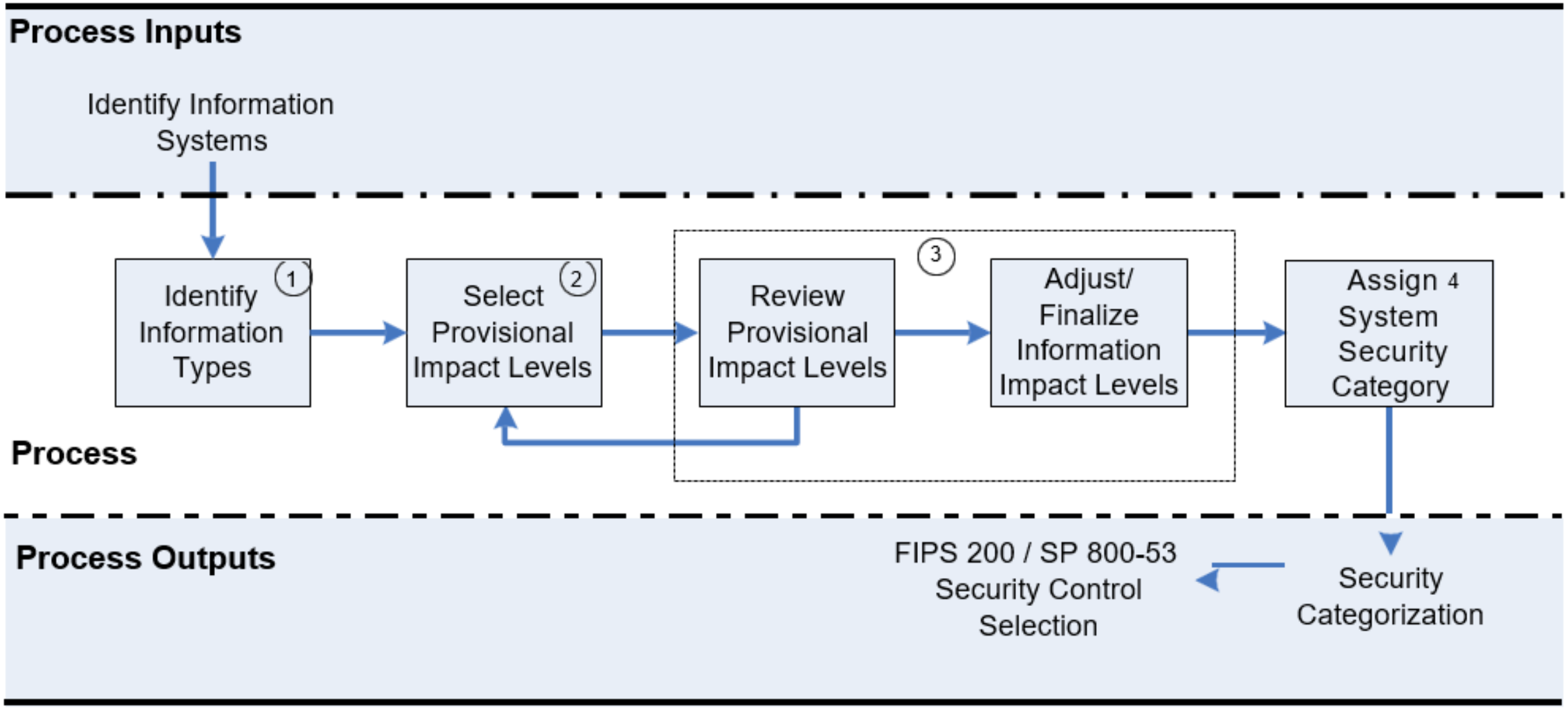
	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 1: FIPS 199 Categorization

Categorization- Potential Impact

- The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. [FIPS 199]

- Security Category information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}



The “Highwater Mark”

	Confidentiality	Integrity	Availability	Result
System A	**High**	Low	Low	High
System B	Low	**Moderate**	Low	Moderate
System C	**Low**	Low	Low	Low
System D	Low	**Moderate**	Low	Moderate
System E	Low	**Low**	Low	Low
System F	Low	Low	**Moderate**	Moderate
System G	Low	**Moderate**	Low	Moderate
System H	**Moderate**	Low	Low	Moderate
System I	Low	**Moderate**	**Moderate**	Moderate

The Categorization is Ultimately Determined

- For Federal agencies, the System Owner makes the ultimate decision concerning the categorization of the system
- Several factors / pieces of information are used
  - Privacy Threshold Analysis (PTA)
  - Business Impact Analysis (BIA)

Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Senior Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

Privacy Impact Assessment (PIA) Guide

This document implements the OPM Information Security and Privacy Policy

Privacy Threshold Analysis (“PTA”)

- Used to determine if a privacy impact assessment (PIA) must be completed
- A properly completed and approved PTA provides documentation indicating that the system owner has accurately assessed whether or not a PIA is required,
- Is an effective tool for analyzing and recording the potential privacy documentation requirements of agency and program activities.
- PTAs should be submitted to an organization’s privacy office for review and approval. PTAs are often comprised of simple questionnaires that are completed by the system owner.
- PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the information security officer, and the information officer.”

Privacy Impact Analysis ("PIA")

- An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Business Impact Analysis (“BIA”)

- A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.
- Potential loss scenarios should be identified during a risk assessment. Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries.
- There are many possible scenarios which should be considered.
- Identifying and evaluating the impact of disasters on business provides the basis for investment in recovery strategies as well as investment in prevention and mitigation strategies.

Business Impact Analysis: Considerations

- Lost sales and income
- Delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay of new business plans

Part II: Risk Management Core
Part 3: The Actual Steps
Subpart : *Select Controls Step*

Select Step, Task 1 – Security and Privacy Requirements Allocation

- Security and privacy requirements are allocated to the system and to the environment in which the system operates.

Select Step, Task 2 – Control Selection

- Control baselines necessary to protect the system commensurate with risk are selected.
- Controls are assigned as system-specific, hybrid, or common controls.

Select Step, Task 3 – Control Tailoring

- Controls are tailored producing tailored control baselines.

Select Step, Task 4 – Security and Privacy Plans

- Security and privacy controls and associated tailoring actions are documented in the security and privacy plans or equivalent documents.

Select Step, Task 5 – Continuous Monitoring Strategy - System

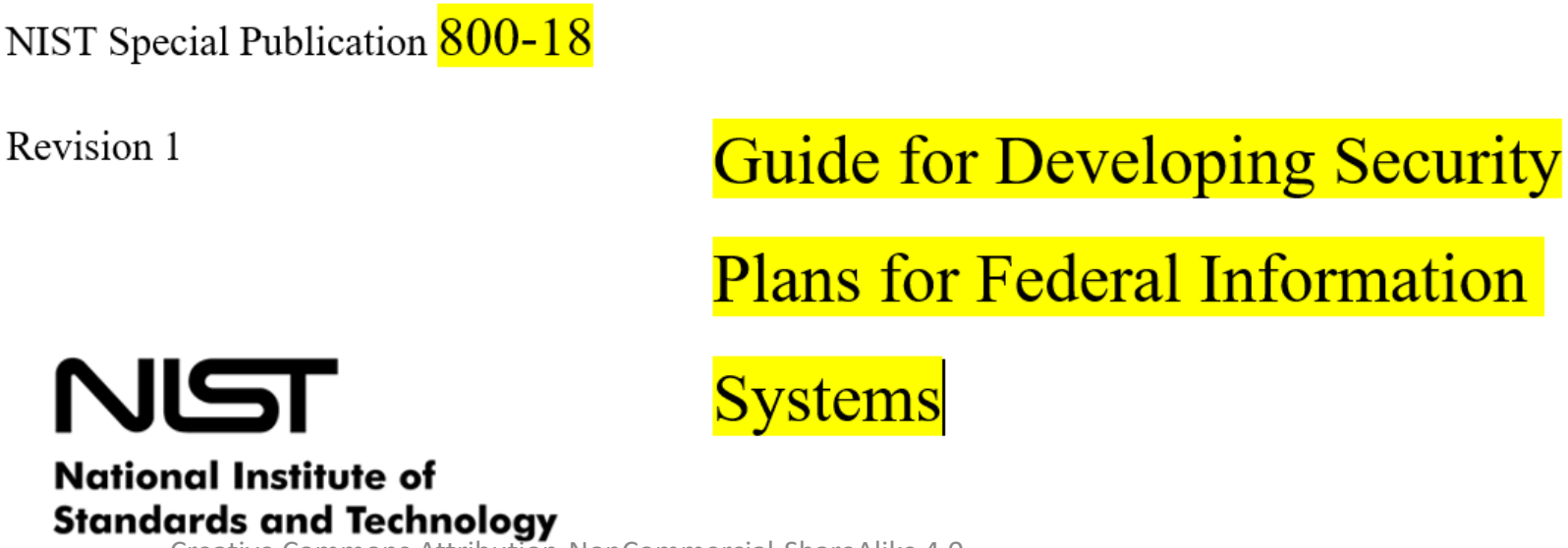
- A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.

Select Step, Task 6 – Security and Privacy Plan Review and Approval

- Security and privacy plans reflecting the selection of controls necessary to protect the system commensurate with risk are reviewed and approved by the authorizing official.

Step 2 – Selecting Security Controls

- Based on the categorization of the system
- Documented in the System Security Plan (Plan)
- NIST 800-18 provides guidance



System Security Plan – The Key Players

- Chief Information Officer
- Information System Owner
- Information Owner
- Senior Agency Information Security Officer (SAISO)
- Information System Security Officer
- Authorizing Official

System Security Plan – The Focus Areas

- System Boundaries
- Major Applications
- General Support Systems
- Minor Applications
- Security Controls

System Security Plan – The Components

- System name and identifier
- System categorization
- System owner
- Authorizing official
- Other designated contacts
- Assignment of security responsibility
- System operational status
- Information system type
- General description/purpose

System Security Plan –Components (cont)

- System environment
- System interconnection/information sharing
- Laws, regulations, and policies affecting the system
- Security control selection
- Minimum security controls
- Completion and approval dates
- Ongoing system security plan maintenance

SSP Development – The Players

- Business Owner
  - The Business Owner has primary responsibility for evaluating the control framework and determining the applicable control for their system and ensuring the proper implementation of the security controls.
- Information System Security Officer (ISSO)
  - Does all of the work on implementing and overseeing (and being audited) on the control

SSP Development – Control Types

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.

Control Enhancements: None.

References: NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-4	**HIGH** PE-4

SSP Development – Control Types (con't)

IR-4 INCIDENT HANDLING

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) *INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*

The organization employs automated mechanisms to support the incident handling process.

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

AU-1: Audit & Accountability Policy & Procedures - Requirements

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Reviews and updates the current:

1. Audit and accountability policy [Assignment: organization-defined frequency]; and

2. Audit and accountability procedures [Assignment: organization-defined frequency].

AU-1: Audit and Accountability Policy and Procedures - Supplemental Guidance

- This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family.
- Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.
- Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary.
- The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.
- The procedures can be established for the security program in general and for particular information systems, if needed.
- The organizational risk management strategy is a key factor in establishing policy and procedures.

AU-1: Audit and Accountability Policy and Procedures: Assessment Procedure

1. Examine Audit and Accountability policy; ensure it addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Ensure it is reviewed and updated at least annually.
2. Examine Audit and Accountability procedures; ensure the procedures include how to implement the Audit And Accountability policy. Ensure they are reviewed and updated at least annually.
3. Validate both the policy and procedures are disseminated to the personnel/roles depicted in the Agency/Organization Policy.

AU-1 Response

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Reviews and updates the current:

1. Audit and accountability policy [Assignment: organization-defined frequency]; and

2. Audit and accountability procedures [Assignment: organization-defined frequency].

AU-2: Audit Events : Req's

a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

AU-2: Audit Events : Assessment Procedure

1. Interview the CISO; determine how auditing functions are coordinated among organizational entities.

2. Interview the SO/ISSO/SA; validate that the system components are capable of auditing the noted events and identify the events that are captured by each system component.

3. For each device in the system boundary, generate screenshot depicting the events that are audited.

4. Examine documentation describing why the selected events are deemed adequate to support after-the-fact investigations.

AU-2: Sample Response

a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

AU-3: Content of Audit Records - Requirement

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

AU-3: Content of Audit Records - Assessment Procedure

1. Interview the SO/ISSO/SA; determine if the audit records contain the noted information.

2. Examine a sample of audit records; validate that the noted information is captured, and generate screenshot.

AU-3: Response by ACME

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

1. Interview the SO/ISSO/SA; determine if the audit records contain the noted information.
2. Examine a sample of audit records; validate that the noted information is captured, and generate screenshot.

WRAPPING UP…CLOSING

- We will cover the remaining steps in another presentation

Part II: Risk Management Core
Part 3: The Actual Steps
Subpart : *Implement Controls* Step

TO BE COVERED IN THE NEXT PRESENTATION

Questions?