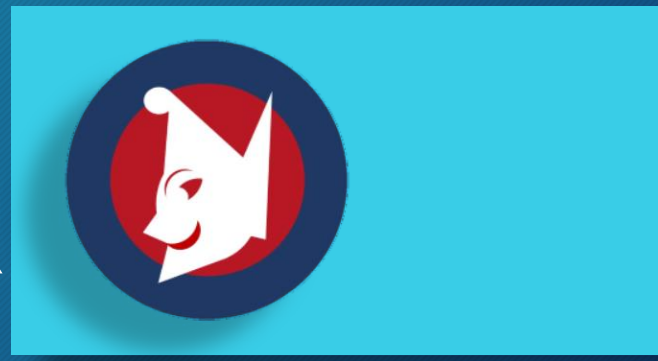
Incorporating Enterprise Priorities to the Risk Management Framework



ISACA-GWDC Presentation 11/2/2017

Noel A Nazario, President
Elfsec LLC

On September 28th, 2017 the National Institute of Standards and Technology (NIST) announced the release of a discussion draft of **Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.**

A key goal of this document is to institutionalize critical enterprise-wide risk management preparatory activities to facilitate a more efficient and cost-effective execution of the Risk Management Framework at the system and operational level.

We will discuss this organizational preparation step and propose implementation strategies that facilitate better communication between system owners, senior leaders and executives at the enterprise and mission/business process levels.

We will also discuss outputs of the organizational preparation step including the clear definition of organizational risk tolerance and acceptable limits for the implementation of security and privacy controls; identification of common controls and the development of organization-wide tailored security and privacy control baselines; reductions to the complexity of the IT infrastructure; and identification of high-value assets and high-impact systems to prioritize their protection

Special Publication 800-37, Revision 2 (Discussion Draft)

- The draft update to the **Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy**
- Next-generation **RMF** in response to **Defense Science Board**, President's **Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**, and the **Office of Management and Budget Memorandum M-17-25** (Cybersecurity Executive Order implementation guidance)
- After the discussion draft, NIST anticipates publishing an initial public draft in November 2017, a final draft in January 2018, and the final publication in March 2018.

Update's Major Objectives

1. Provide closer linkage and communication between the risk management processes and activities at the C-suite level of the organization and the processes and activities at the system and operational level of the organization;
2. Institutionalize critical enterprise-wide risk management preparatory activities to facilitate a more efficient and cost-effective execution of the Risk Management Framework at the system and operational level;
3. Demonstrate how the Cybersecurity Framework can be implemented using the established NIST risk management processes (i.e., developing a Federal use case); and
4. Provide an integration of privacy concepts into the Risk Management Framework and support the use of the consolidated security and privacy control catalog in NIST Special Publication 800-53, Revision 5.

Key Change: The Preparation Step

Aims to achieve more effective, efficient, and cost-effective risk management processes. Its primary objectives are:

1. Better communication among enterprise leadership, mission/business process leaders, and system owners to convey acceptable security and privacy controls implementation constraints and organizational risk tolerance
2. Help identify organization-wide common controls and develop organization-wide tailored security and privacy control baselines to reduce individual system owner workload and system development and protection costs

Key Change: The Preparation Step

3. Reduce IT infrastructure complexity by consolidating, standardizing, and optimizing systems, applications, and services through the application of enterprise architecture concepts and models
4. Identify, prioritize, and focus resources on high-value assets and high-impact systems that require increased levels of protection, while moving lower-impact systems to cloud or shared services, systems, and applications

Note: Part of the exercise is to base any decisions on enterprise-level direction informed by risk assessments and awareness of the dependencies among systems to avoid low-impact systems to open high-value assets to attack.

Using the Cybersecurity Framework

- Executive Order (E.O.) 13800 requires federal agencies to modernize their IT infrastructure and systems, agency heads are to manage risk using the **Framework for Improving Critical Infrastructure Cybersecurity** (aka, the Cybersecurity Framework). EO reinforces FISMA (2014) by holding agency heads accountable for managing their enterprise cybersecurity risk.
- The Cybersecurity Framework can be used with various cybersecurity risk management processes. The Federal Use Case requires agencies to implement CSF using the processes defined SP 800-37 and SP 800-39 **Managing Information Security Risk – Organization, Mission, and Information System View**.

Cybersecurity Framework Federal Implementation

- The federal implementation of the Cybersecurity Framework will focus on —
  - the ***preconditions*** and essential activities necessary to prepare for the enterprise-wide execution of the RMF and the conduct of the associated risk management actions at the information system level; and
  - the ***postconditions*** and essential activities necessary to report the findings and risk-based decisions of authorizing officials for information systems and common controls to agency heads and the senior leaders in the Executive Branch.

RMF Step 0

RMF Steps 3 - 6

Cybersecurity Framework Federal Implementation

Each task in the RMF includes references to applicable sections of the Cybersecurity Framework. For example,

- Organizational Preparation: Task 2 *Risk Management Strategy* - Provides a direct linkage to the Cybersecurity Framework Core [Identify Function]
- Organizational Preparation: Task 10 *Organization-Wide Tailored Control Baselines and Profiles* - Aligns with the construct of Cybersecurity Framework Profiles
- Authorization: Task 6: *Authorization Reporting*, and Task 5: *Security Status Reporting* - Support OMB risk management and status reporting requirements using the Cybersecurity Framework functions, categories, and subcategories.

Wholistic View of Cyber Risk Management

In organizations that depend on information technology for their mission/business success, security and privacy decisions cannot be made in isolation—rather, such decisions are closely linked to decisions regarding

- the mission and business objectives of the organization;
- the modernization of information systems, components, and services to adopt new and innovative technologies;
- the enterprise architecture and the need to manage and reduce the complexity of systems through consolidation, optimization, and standardization (i.e., reducing the attack surface and technology footprint exploitable by adversaries); and
- the allocation of resources to ensure the organization can conduct its missions and business operations with a high degree of effectiveness, efficiency, and cost-effectiveness.

Streamlining RMF Implementation

1. Maximize use of organization level *common controls* to promote inheritance of standardized, consistent, and cost-effective security and privacy capabilities
2. Maximize use of *shared* or *cloud-based* systems, services, and applications to reduce the number of ATOs
3. Use organization-wide *tailored* control baselines to increase focus, consistency, and faster development of security and privacy plans
4. Establish and publicize organization-wide *control parameters* for greater consistency and faster development of security and privacy plans
5. Maximize the use of *automated tools* to implement the RMF and related processes

Streamlining RMF Implementation

6. Decrease level of effort and cost for *low-impact* systems if those systems cannot adversely affect higher-impact systems through system connections
7. Maximize *reuse* of RMF artifacts as appropriate CAUTION!
8. Reduce IT infrastructure *complexity through least functionality* principle and elimination of unnecessary systems, components, and services
9. Reduce cost and increase security and privacy program efficiency through quick transition to *ongoing authorization* and *continuous monitoring* approaches
10. Use common sense security and privacy controls by *rightsizing* RMF activities

RMF and Organization-Wide Risk

A three-level approach to risk management that addresses risk-related concerns at the *organization* level, the *mission/business process* level, and the information *system* level (800-39)

CSF – RMF Implementation: Preparation

The activities conducted at Levels 1 and 2 are critical to preparing the organization to execute the RMF.

Preparation involves activities that go beyond security, but are essential to achieving adequate security and appropriate risk management.

- Level 3 addresses risk from a *system* perspective and is guided and informed by the risk decisions at the enterprise and mission/business process levels.

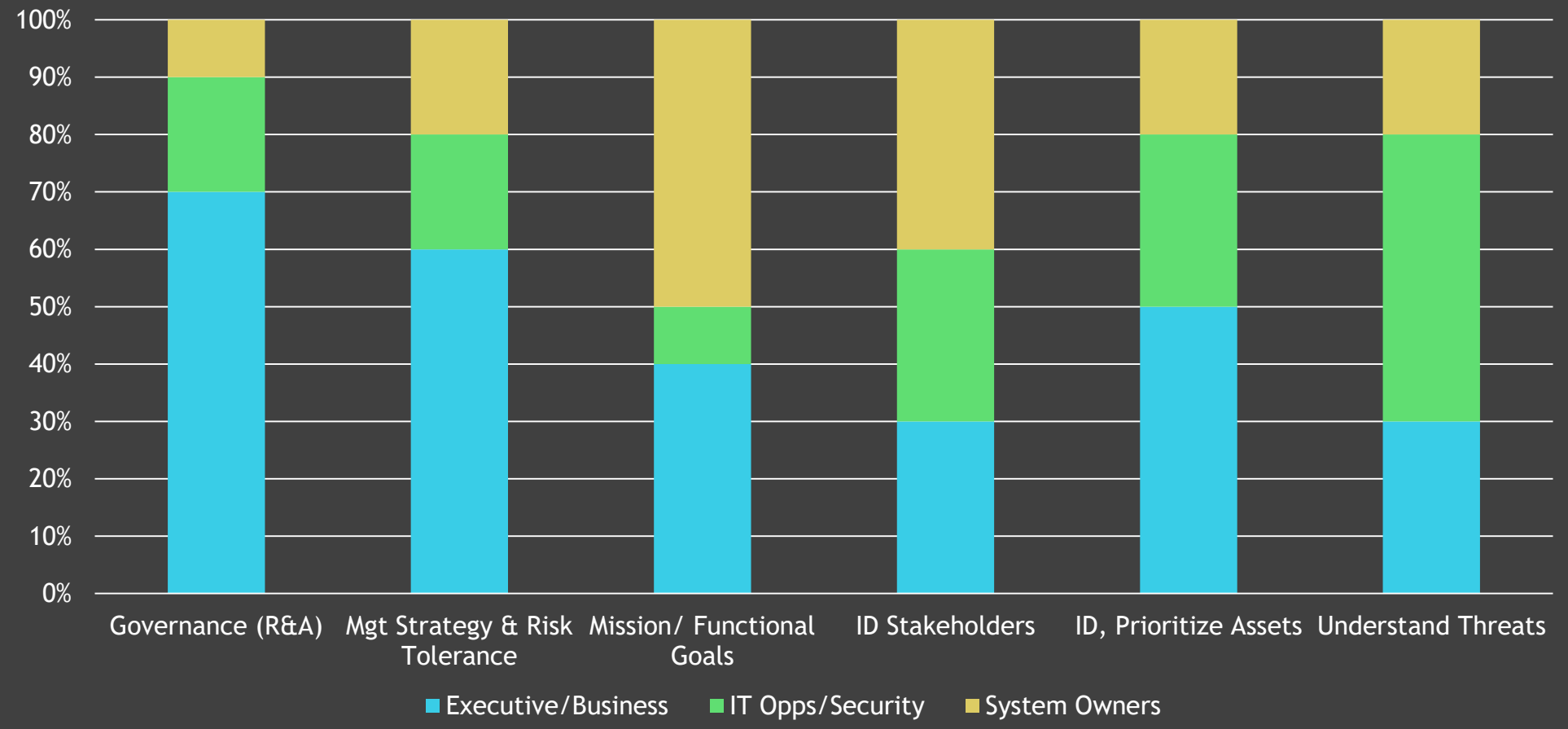
Preparation Activities

1. Assigning key roles and responsibilities for risk management processes;
2. Establishing a risk management strategy and risk tolerance for the organization;
3. Identifying the missions, business functions, and mission/business processes the information system is intended to support;
4. Identifying key stakeholders (both internal and external to the organization) having a security or privacy interest in the information system;
5. Identifying and prioritizing stakeholder assets;
6. Understanding threats to systems and organizations;

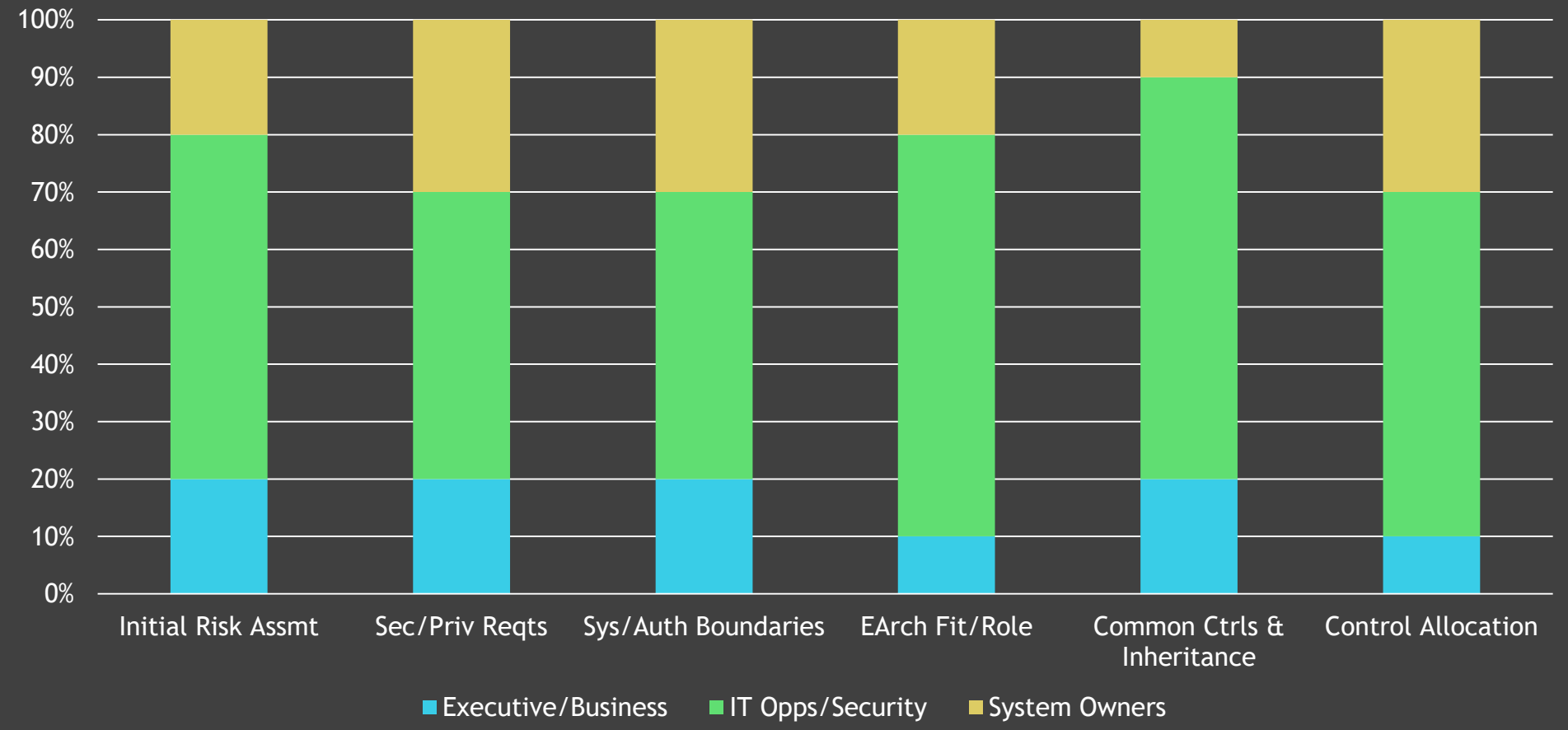
Preparation Activities

7. Conducting an initial risk assessment;
8. Identifying and prioritizing stakeholder protection needs and security and privacy requirements;
9. Determining information system and authorization boundaries;
10. Defining information systems in terms of the enterprise architecture;
11. Developing security and privacy architectures that include common controls suitable for inheritance by organizational systems; and
12. Allocating security and privacy requirements to individual systems and the environments in which those systems operate.

Assignment of Preparation Activities



Preparation Activities



Enterprise Architecture

A strategic information asset base, that defines

- the mission;
- the information and the technologies necessary to perform the mission; and
- the transitional processes for implementing new technologies in response to changing mission needs.

Enterprise architecture includes a baseline architecture, target architecture, and sequencing plan.

Enterprise Architecture

- Organizations that fail to define and implement an effective enterprise architecture strategy will not be able to consolidate, optimize, and standardize the information technology infrastructure—resulting in unnecessary redundancy and inefficient and costly systems, applications, and services.
- Ill-conceived architectural and design decisions can produce a cost-multiplier effect downstream that adversely impacts the ability of the organization to implement effective security and privacy solutions.

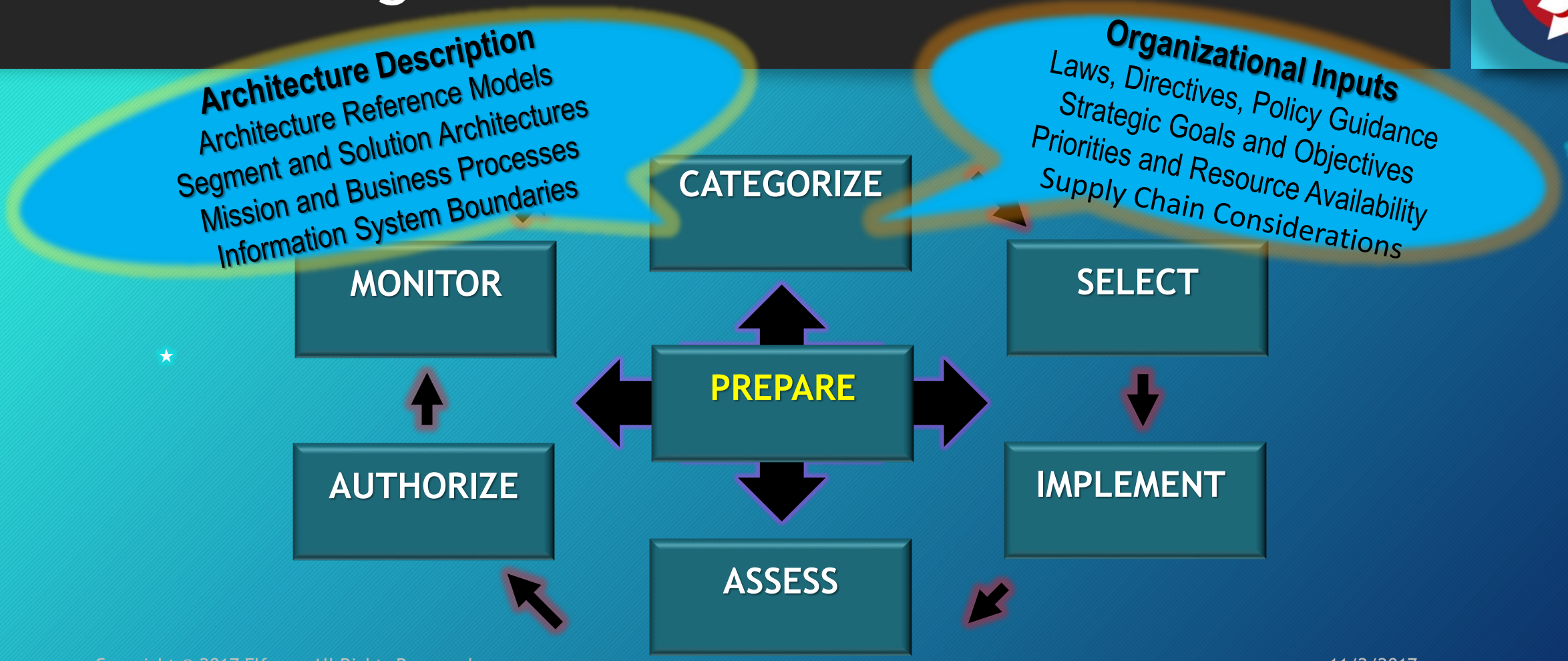
Control Allocation

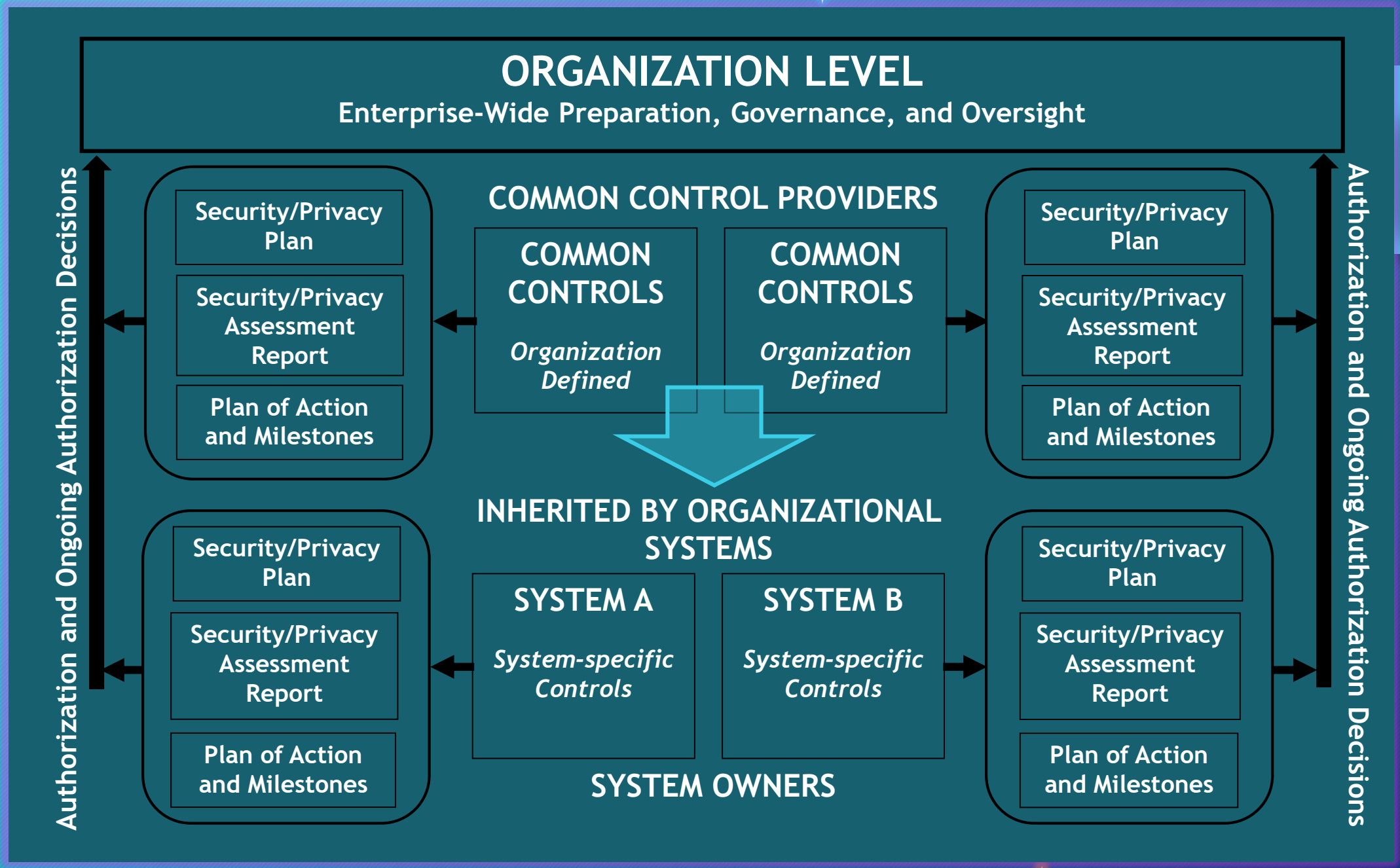
A term used to describe the process an organization employs:

i. to determine whether security controls are defined as system-specific, hybrid, or common; and

ii. to assign security controls to specific information system components responsible for providing a particular security capability (e.g., router, server, remote sensor).

Risk Management Framework





Re-Cap

- Preparation is key to obtaining value from your cyber risk management program
- Implementation of the Cybersecurity Framework is the US Government's goal. The Practice Case for the Federal Implementation of the CSF relies on implementation of Risk Management Framework per EO and OMB Guidance.
- Executive leadership must be involved in cyber risk management; it is incumbent on us to provide the right information and work cooperatively to obtain strategic guidance and support.
- Proper implementation and common sense application of the guidance are the key to positive return on investment.

Noel A Nazario
President, Elfsec LLC

Http://elfsec.com

Info@Elfsec.com
202-812-8352