The Evolving Risk Management Framework for Ground Systems

Daniel P. Faigin, CISSP
The Aerospace Corporation

Evolution of Ground System Architectures

- 1980s/1990s:
  Stove-Piped Ground Systems
- 1990s/2000s:
  Distributed Networked Ground Systems with Isolated Networks
- 2000s/2010s:
  Distributed Networked Ground Systems on the GIG

Ground Systems are increasingly networked and connected to outside networks

Evolution of the Threats

- 1980s/1990s:
  - *Physical*
  - *Insider*
- 1990s/2000s:
  - *Physical*
  - *Insider*
  - ***Remote Access***
  - ***Network Attack***
- 2000s/2010s:
  - *Physical*
  - *Insider*
  - *Remote Access*
  - *Network Attacks*
  - ***Cyber Attacks***
    - **Determined Nation-States**
    - **Sophisticated Hackers**
    - **"Script Kiddies"**

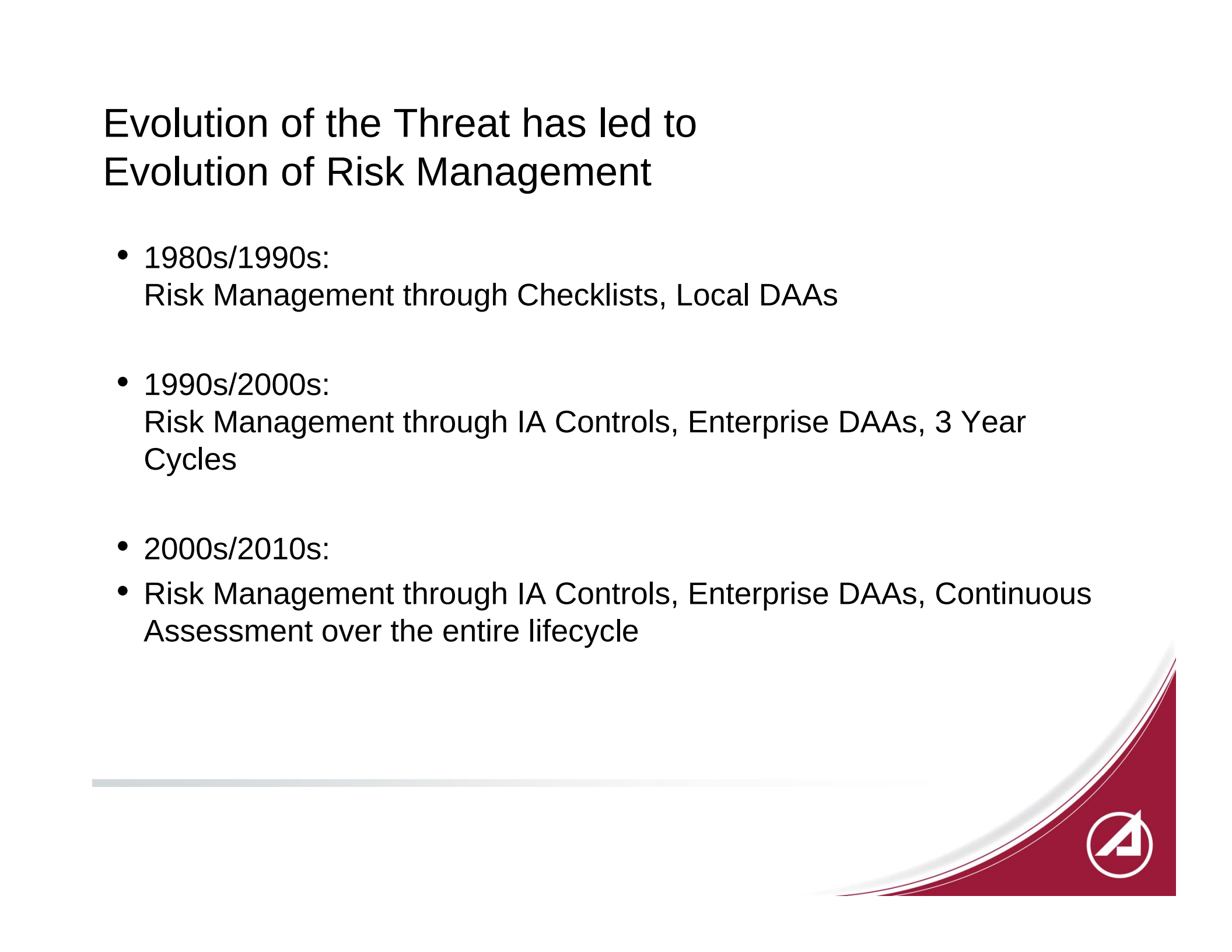
Attackers have become increasingly sophisticated and adept

Evolution of the Threat has led to Evolution of Risk Management

- 1980s/1990s:
  Risk Management through Checklists, Local DAAs

- 1990s/2000s:
  Risk Management through IA Controls, Enterprise DAAs, 3 Year Cycles

- 2000s/2010s:
- Risk Management through IA Controls, Enterprise DAAs, Continuous Assessment over the entire lifecycle



Changing Goals

- The goals have changed as well:
  - *Confidentiality →*
    Confidentiality, Integrity, Availability
  - *Information Protection →*
    Information Protection / Sharing
  - *Static, Point-in-Time Focus →*
    Dynamic, Continuous Monitoring Focus
  - *Government-Centric Solutions →*
    Commercial Solutions
  - *Risk Avoidance →*
    Risk Management

Joint Task Force Transformation Initiative

- Created in 2009 to transform the processes
- Represents a broad-based partnership:
  - *National Institute of Standards and Technology*
  - *Department of Defense*
  - *Intelligence Community*
    - Office of the Director of National Intelligence
    - 16 U.S. Intelligence Agencies
  - *Committee on National Security Systems*
- Goal: Produce a Unified Information Security Framework for the federal government

Unified Framework Provides a Common Approach

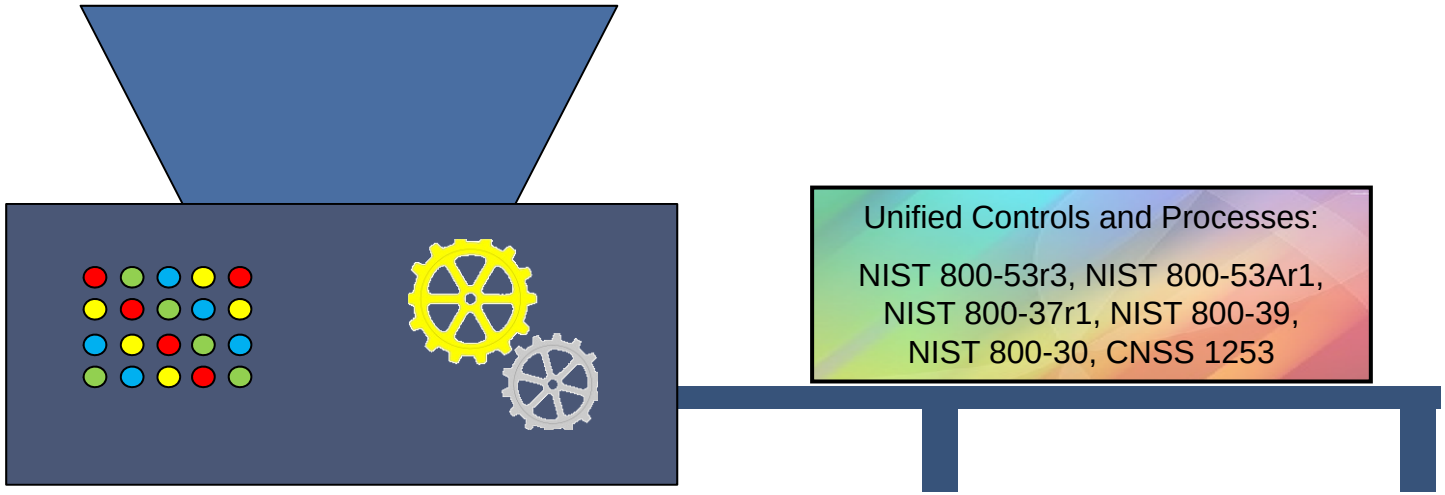
NIST Information Security Standards and Guidance

- Risk management (organization, mission, system)
- Security categorization (information criticality/sensitivity)
- Security controls (safeguards and countermeasures)
- Security assessment procedures
- Security authorization process

Intelligence Community Controls

Department of Defense Controls

Federal/Civil Agency Controls

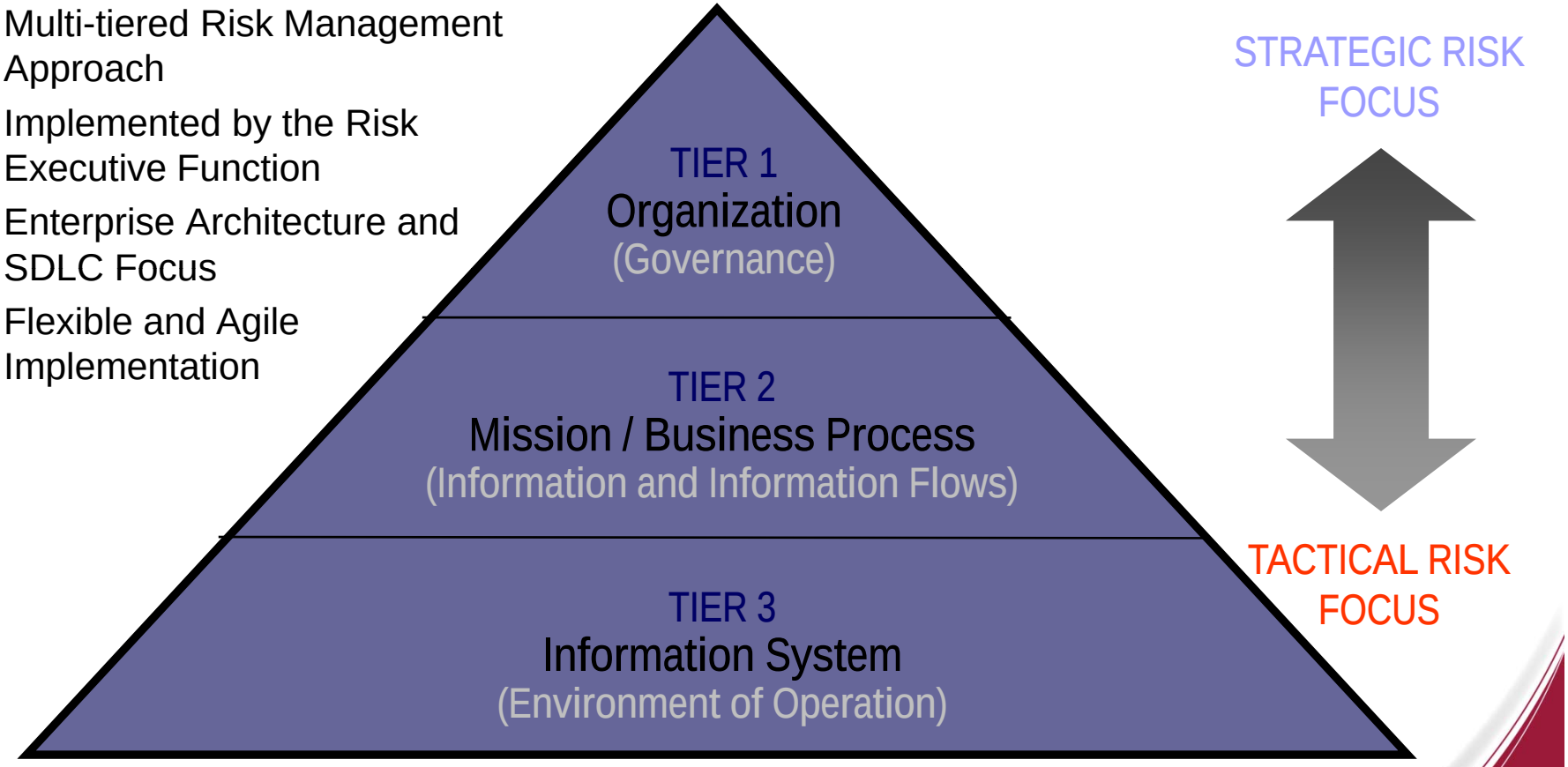


Unified Controls and Processes:

NIST 800-53r3, NIST 800-53Ar1, NIST 800-37r1, NIST 800-39, NIST 800-30, CNSS 1253

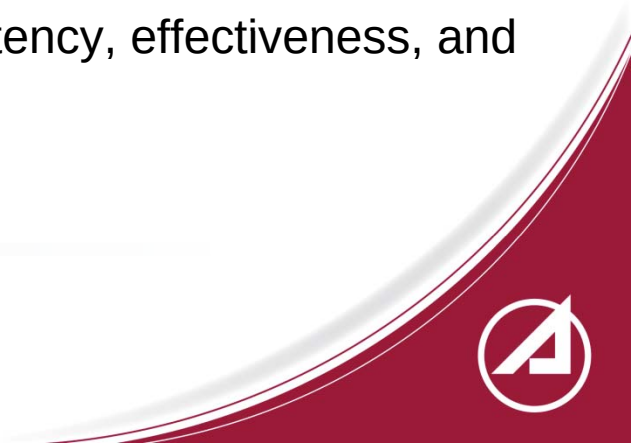
Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



Characteristics of Risk-Based Approaches

- Integrates information security into the enterprise architecture and system life cycle.
- Promotes near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes.
- Provides senior leaders with necessary information to make risk-based decisions regarding information systems supporting their core missions and business functions.
- Links risk management activities at the organization, mission, and information system levels through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within information systems.
- Encourages the use of automation to increase consistency, effectiveness, and timeliness of security control implementation.



Risk Management Lifecycle (DIACAP)

Decommission System

1 Initiate and Plan IA C&A

- **Register with DoD Component IA Program**
- **Assign IA Controls**
- **Assemble DIACAP Team**
- **Initiate DIACAP Implementation Plan**

5 Decommission

- **Retire System**

DoD Information Systems

- *AIS Applications*
- *Enclaves*
- *Platform IT Interconnection*
- *Outsourced IT-Based Processes*

2 Implement and Validate Assigned IA Controls

- **Execute DIACAP Implementation Plan**
- **Conduct Validation Activities**
- **Prepare POA&M**
- **Compile Validation Results in DIACAP Scorecard**

4 Maintain Authority to Operate and Conduct Reviews

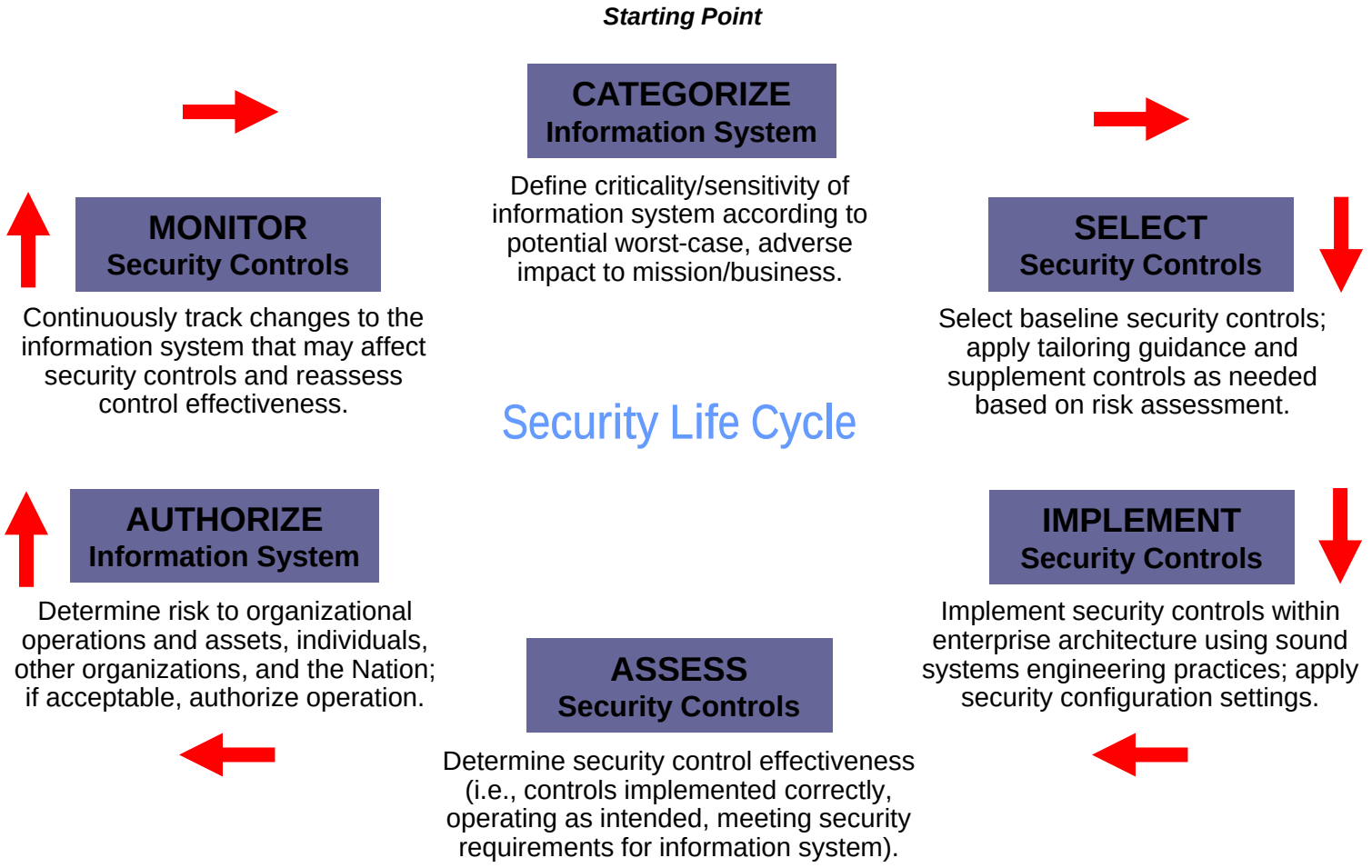
- **Maintain Situational Awareness**
- **Maintain IA Posture**
- **Conduct Reviews (Review of IA Controls must occur at least annually)**
- **Initiate Re-accreditation**

3 Make Certification Determination & Accreditation Decision

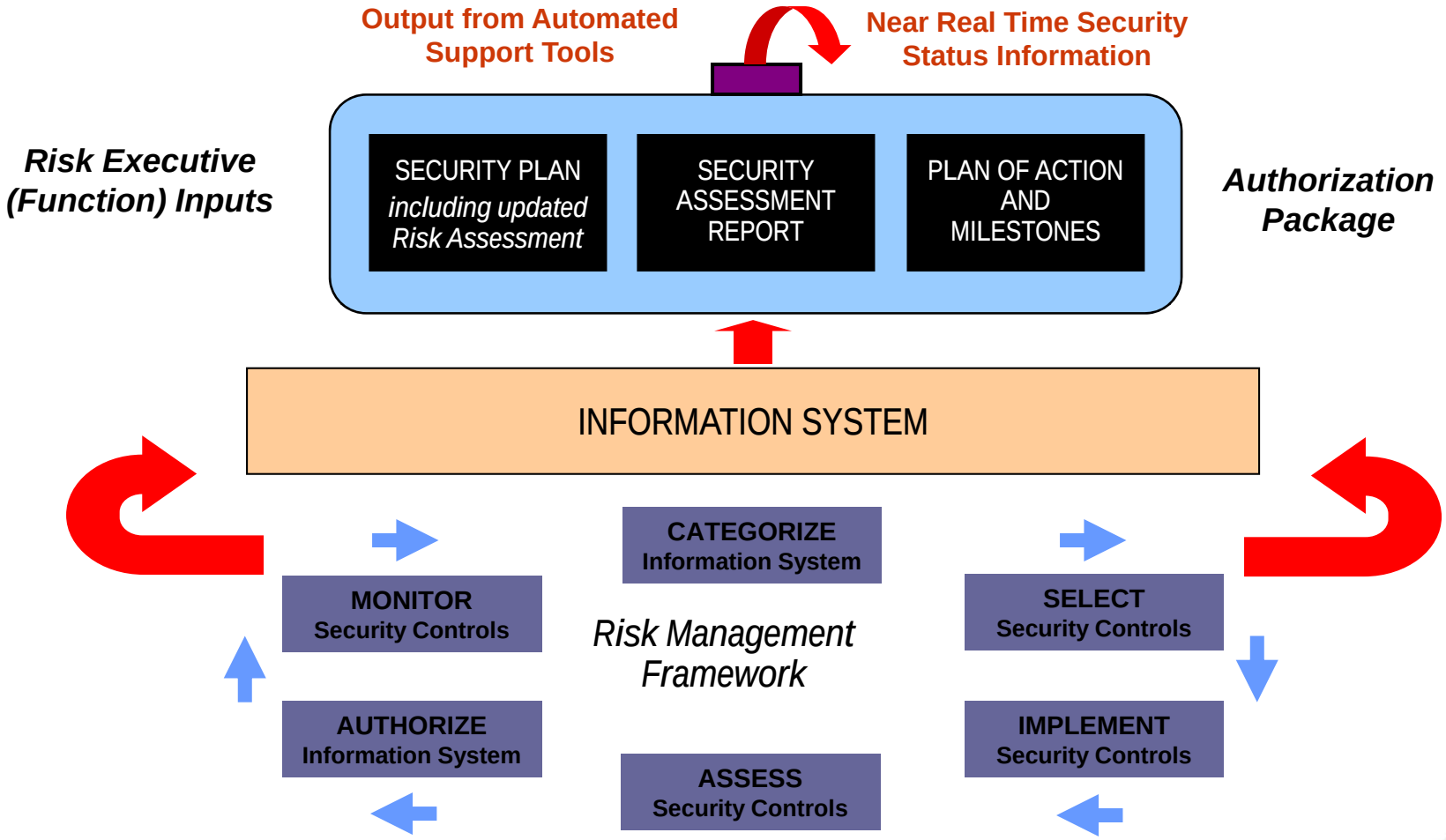
- **Make Certification Determination**
- **Issue Accreditation Decision**

Graphics courtesy of OASD (NII)

Risk Management Lifecycle (NIST 800-37)

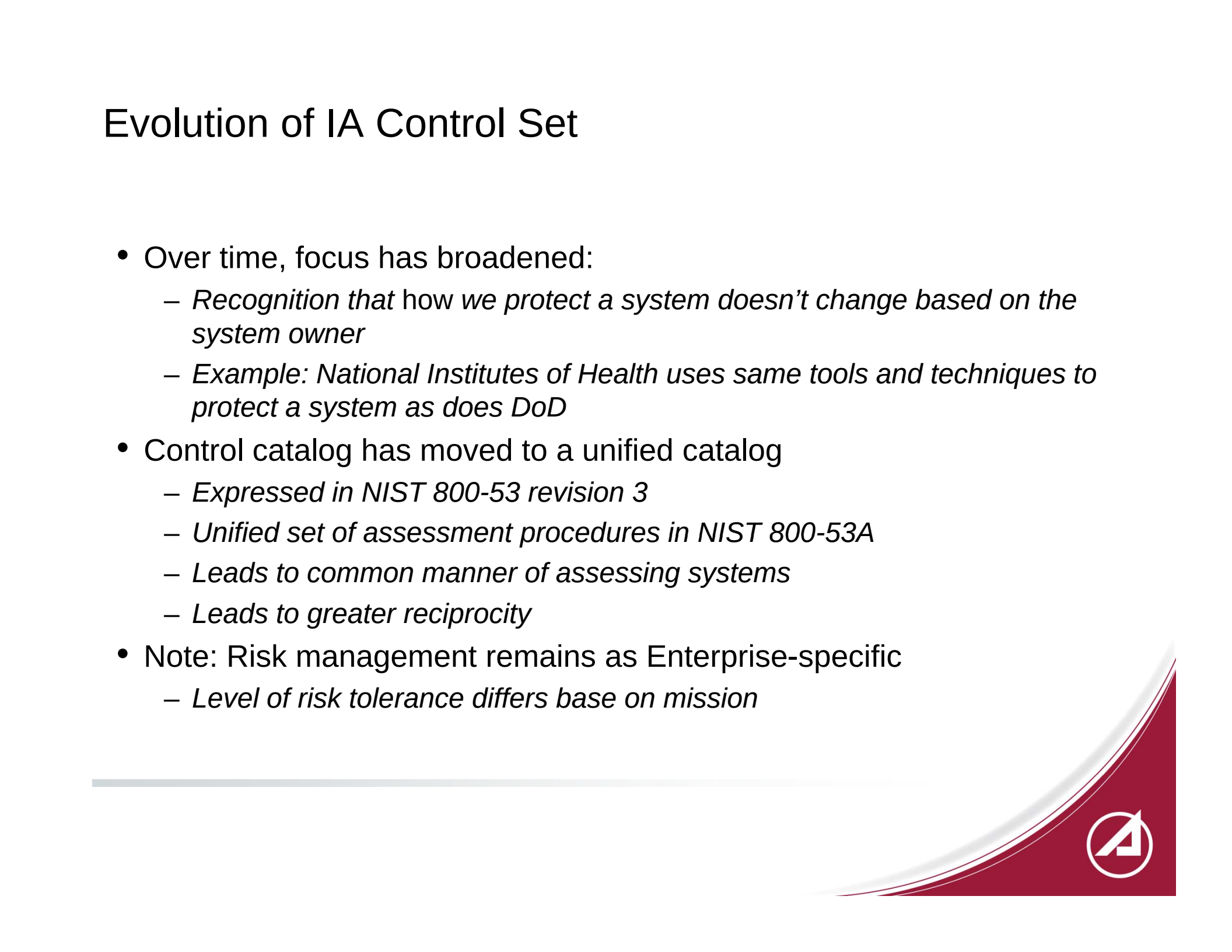


Deliveries are Similar Between the Processes



Evolution of IA Control Set

- Over time, focus has broadened:
  - *Recognition that* how *we protect a system doesn't change based on the system owner*
  - *Example: National Institutes of Health uses same tools and techniques to protect a system as does DoD*
- Control catalog has moved to a unified catalog
  - *Expressed in NIST 800-53 revision 3*
  - *Unified set of assessment procedures in NIST 800-53A*
  - *Leads to common manner of assessing systems*
  - *Leads to greater reciprocity*
- Note: Risk management remains as Enterprise-specific
  - *Level of risk tolerance differs base on mission*



Categorization of Information Systems (DOD 8500.1/DIACAP)

- All DoD information systems are assigned a mission assurance category (MAC) and confidentiality level (CL).
- Requirements for availability and integrity are associated with the mission assurance category
- Requirements for confidentiality are associated with the information classification or sensitivity and need-to-know.
- The MAC and CL determine the baseline set of IA controls

DoDD 8500.1, Section 4.7

Categorization in the Transformational Era

- Based off of **Impact Levels**:

FIPS 199	LOW	MODERATE	HIGH
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Categorization in the Transformational Era

- Non-National Security Systems (NSS) use the **High Water Mark** of the C/I/A Impact Levels
- NSS have a distinct impact level in each category
- For NSS, the categorization will likely be further modified by:
  - *Accessibility*
    - Profiles based on relationship between classification of data and clearance of users
  - *Classification*
    - Overlays based on actual classification levels
  - *Application*
    - Overlays based on special uses: cross domain, tactical, space

IA Controls are Grouped by Subject Area

- Eight (8) Subject Areas in DOD 8500.2:

Abbreviation	Subject Area Name	Number of Controls in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

- 157 total controls

IA Controls are Grouped by Subject Area

- Eighteen (18) Subject Areas in NIST 800-53:

ID	FAMILY	CLASS	# OF CTLS/ENH
AC	Access Control	Technical	86
AT	Awareness and Training	Operational	8
AU	Audit and Accountability	Technical	44
CA	Security Assessment and Authorization	Management	13
CM	Configuration Management	Operational	42
CP	Contingency Planning	Operational	43
IA	Identification and Authentication	Technical	33
IR	Incident Response	Operational	21
MA	Maintenance	Operational	23
MP	Media Protection	Operational	19
PE	Physical and Environmental Protection	Operational	47
PL	Planning	Management	8
PS	Personnel Security	Operational	12
RA	Risk Assessment	Management	13
SA	System and Services Acquisition	Management	41
SC	System and Communications Protection	Technical	94
SI	System and Information Integrity	Operational	53
PM	Program Management	Management	11

- Note: PM controls do not apply to NSS

IA Controls are Grouped by Subject Area

- Roughly equivalent to DOD 8500.2, but finer-grained
  - *600 controls + enhancements vs. 157*
- Controls are structured differently
  - *No hierarchy of controls (e.g. ECCR-1 < ECCR-2 < ECCR-3)*
  - *Controls are structured as a base control (AC-2) plus enhancements (AC-2(1)(3))*
    - Enhancements are effectively additional control statements related to the base control

Example: EBRU-1
Remote Access for User Functions

- "All remote access to DOD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected."

DoDI 8500.2

Example Control: AU-5

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects; delays*] network traffic above those thresholds.

4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

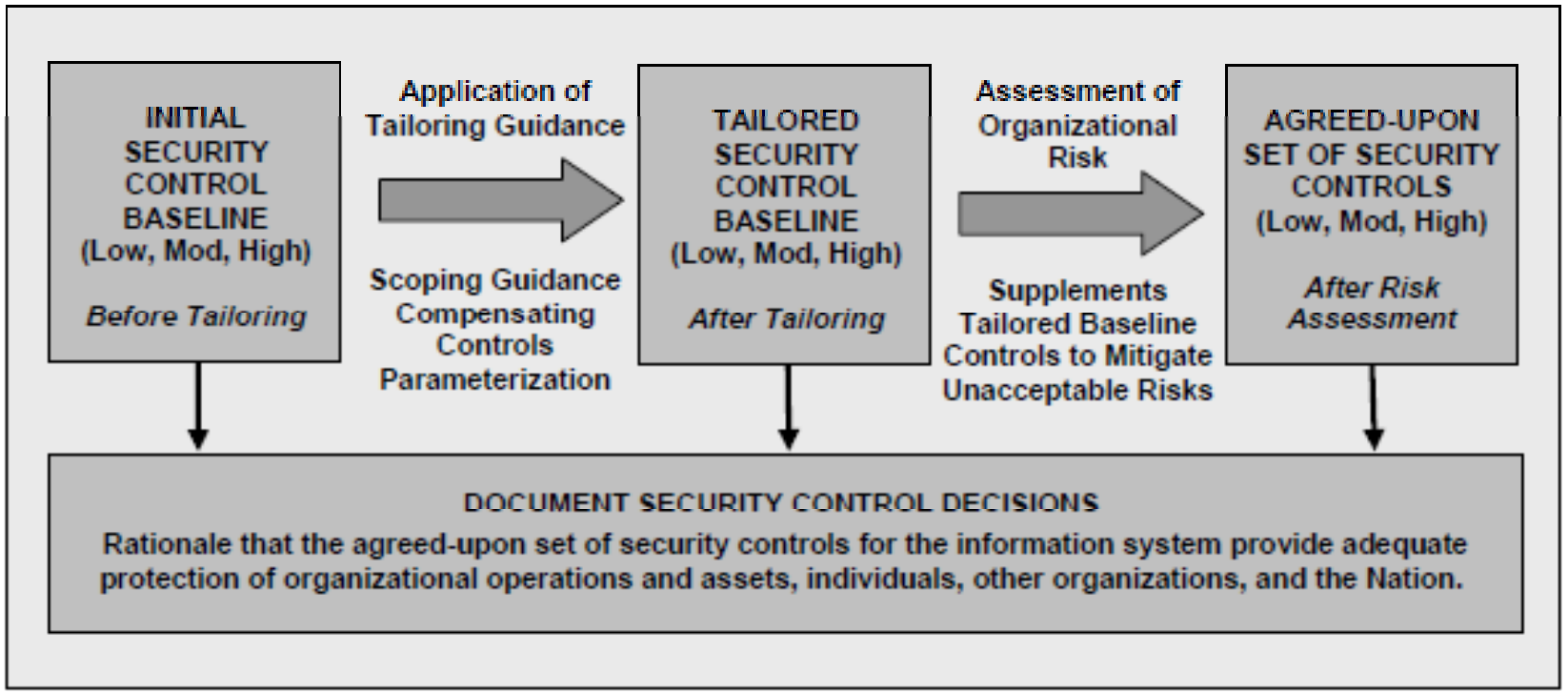
Priority and Baseline Allocation: P1 **LOW** AU-5 **MOD** AU-5 **HIGH** AU-5 (1) (2)

CNSS 1253 interacts with NIST 800-53

- CNSS 1253 defines the NSS baselines:
  - *For AU-5:* *Confidentiality – Not Selected*
    Integrity – Not Selected
    Availability – Low, Moderate, High
- CNSS 1253 completes some assignments:
  - *For AU-5(1): "or a maximum of 75%"*
- It is anticipated that the upcoming CNSS 1253 revision or updated DOD guidance will:
  - *Correct some baselining problems*
  - *Complete a larger percentage of assignments/selections*

The Security Control Selection Process

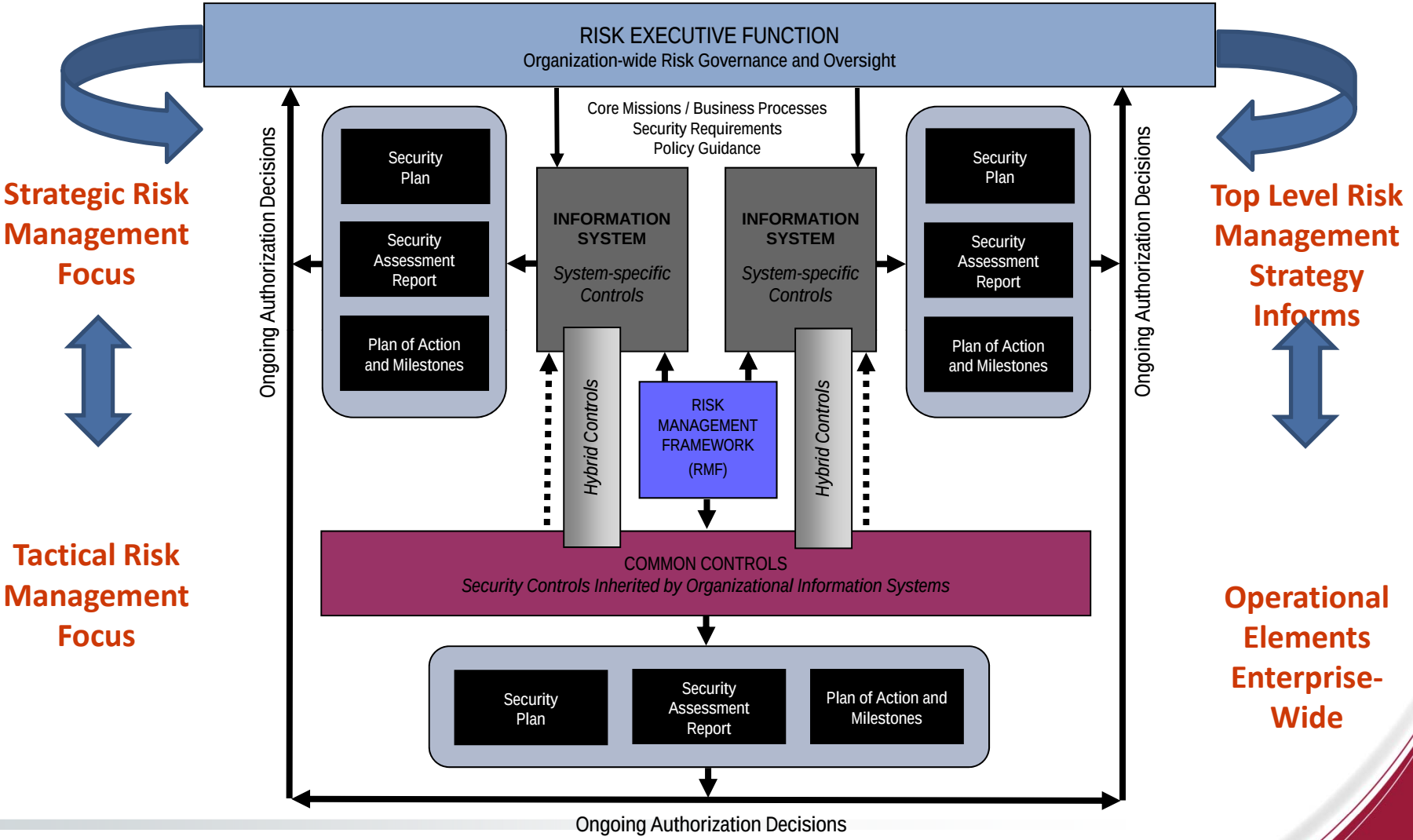
- Selection doesn't just stop at the baseline
- Important to tailor controls based on additional needs



Security Control Allocation

- Security controls are defined to be system-specific, hybrid, or common.
- Security controls are allocated to specific components of organizational information systems as system-specific, hybrid, or common controls.
- Security control allocations are consistent with the organization's enterprise architecture and information security architecture.

Security Control Accountability



Learning More Information: Transformational Documents

NIST SP 800-53	**Recommended Security Controls for Federal Information Systems and Organizations** Revision 3 (August 2009) + Errata as of May 1, 2010 *Revision 4 planned for late 2011*
NIST SP 800-53A	**Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans** Revision 1 (June 2010)
NIST SP 800-37	**Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach** Revision 1 (February 2010)
NIST SP 800-30	**Guide for Conducting Risk Assessments** *Revision 1 scheduled for March 2011*
NIST SP 800-39	***Enterprise-wide Risk Management: Organization, Mission, and Information Systems View*** *Revision 1 scheduled for February 2011*
CNSS 1253	***Security Categorization and Control Selection for National Security Systems*** October 2009 *Revision anticipated in 2011*

NIST documents available at:
http://csrc.nist.gov/publications/PubsSPs.html
CNSS documents available at:
http://www.cnss.gov/instructions.html
FISMA Project Implementation Schedule:
http://csrc.nist.gov/groups/SMA/fisma/schedule.html

When Can I Expect This:

- ~6 mo post: DoD states it will issue updates to 8500.1/8500.2
- ~9 mo post: DoD states it will issue updates to 8510.1
- ICD 503 already points to NIST documents
  - *DCID 6/3 used operationally until transformational documents complete*

- Additional complicating factor:
  - *NIST 800-53 revision 4 anticipated late 2011/2012*

Credits and Contacts

- Thank You to Dr. Ron Ross of NIST for permitting me to extract information from his slides presented at ACSAC 2009

- Speaker Contact:
  - *Daniel P. Faigin*
    The Aerospace Corporation
    faigin@aero.org