Audit Interactive

A Higher Education Collaborative Experience

March 9-12, 2025 | Sheraton Hotel Downtown | Oklahoma City, OK

ACUA
Association of College & University Auditors

How to Audit a Cybersecurity Maturity Model Certification (CMMC) Program

Presenter Johan Lidros
CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, CDPSE, ITIL-F
President Eminere Group

Introduction

The Office of the Department of Defense Chief Information Officer (CIO), Department of Defense (DoD) issued the final rule for Cybersecurity Maturity Model Certification (CMMC) Program in October 2024.

Many other federal agencies are working to define similar approaches for federal grants or services due to the increased threat level.

We will discuss the roles an internal audit function can play in the CMMC journey, how to perform a pre-assessment, and how to audit certain more challenging areas of the requirements with the help of case studies and practical examples.

Main Session Objectives

1. Define approach to audit/assess a higher educations CMMC program from an internal audit perspective
2. Demonstrate knowledge of the assessment of key control areas defined in the CMMC requirements.
3. Identify key strengths and opportunities in the CMMC program.
4. Understand the CMMC integration with the institution's IT governance and Information security programs.

Presenter

Johan Lidros, Founder and President of Eminere Group

- Over 30 years of experience providing information technology audit, security, privacy, compliance and IT governance services in for many healthcare and higher education institutions. Johan has worked with more than 100 universities in the US and northern Europe.
- Well-versed in accepted IT and information security standards/frameworks (ISO27000, HITRUST, NIST, COBIT, CIS, TIR, DRII, etc.) and has participated in several related committees.
- Certifications: CISA, CISM, CGEIT, CDPSE, ITIL-F, CRISC, HITRUST CCSFP
- ISACA certified instructor CISA, CISM, CRISC, CGEIT

Research Overview

- Research is defined as the systematic investigation into and study of materials and sources in order to establish facts and reach conclusions.
- Research includes scientific computations, scientific lab studies, psychology evaluations, observations, surveys, testing, clinical trials and more.
- Research extends beyond federal funding and has expanded into more areas including environmental, space and sustainability.
- There is increased scrutiny over research activities, reporting integrity, and how dollars are spent.
- Expectations are greater for institutions efforts for security, data protection, and the use of AI in research.
- There is a greater demand for the recruitment of research subjects.

Agenda

- Introduction
- History and Background
- The Audit Perspective – Audit Approach
- Key Challenges
- Root Causes
- Conclusion
- Resources
- Q&A

- The U.S. government and States are racing towards adoption of new cybersecurity standards.
- There are common themes:
  - Require certification of products and services (the U.S. already has the FedRAMP and StateRAMP program for cloud service providers if U.S. government information is involved).
  - Require Attestation
- Require reporting of cybersecurity incidents within a certain time covering different sectors

- U.S. (cybersecurity) requirements can come from:
  - Local governments (local laws/regulations)
  - State governments (state laws/regulations)
  - Executive Orders issued by the President (which can become regulations)
  - Statutes passed by Congress and signed by the President (which can become regulations).

- Laws or regulations can focus on security, privacy, compliance or enforcing criminal compliance.

- Internationally Views Cybersecurity – Research
  - Security/privacy laws
  - ISO Certifications
  - CISA Audits
  - Attestations
  - UK - “UK Defence Supply Base” (DSB)
  - Canada - Contract Security Program (CSP)
  - Etc.

New Cybersecurity Initiatives

NEW Federal Acquisition Regulation (FAR) Cybersecurity Proposed Rule: Incident Notifications

Proposed Rule: "DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to increase the sharing of information about cyber threats and incident information between the Government and certain providers, pursuant to Office of Management and Budget recommendations…"

Requires:

- Security incident reporting within eight hours (and follow-ups every 72 hours)
- Definition of "incident" very broad
- Must allow government access to compromised systems
- Contractors must develop and maintain a software bill of materials

Likely finalized as a rule in early 2025

New Cybersecurity Initiatives

NEW FAR Cybersecurity Proposed Rule: Governmentwide Cybersecurity Controls

- Proposed Rule: Implements NIST 800-171 for the protection of Controlled Unclassified information (CUI) across the Government.
- Notice of Proposed Rulemaking NPRM was released in 2024 with a final rule in 2025.

New Cybersecurity Initiatives

Cybersecurity Infrastructure Security Agency (CISA)

- CISA released proposed regulations in April 2024.
- 72 hours to report an incident and 24 hours to report a ransomware payment.
  - Critical infrastructure companies are included in requirement – definition is broad and includes wide swath of contractors.
  - Some small businesses are excluded – but not defense sector small businesses or IT government contractors.
  - Exclusions for “substantially similar” reporting requirements. Unknown what qualifies at this time.

New Cybersecurity Initiatives

Cybersecurity Infrastructure Security Agency (CISA)

- CISA released proposed regulations in April 2024.
- 72 hours to report an incident and 24 hours to report a ransomware payment.
  - Critical infrastructure companies are included in requirement – definition is broad and includes wide swath of contractors.
  - Some small businesses are excluded – but not defense sector small businesses or IT government contractors.
  - Exclusions for “substantially similar” reporting requirements. Unknown what qualifies at this time.

New Cybersecurity Initiatives

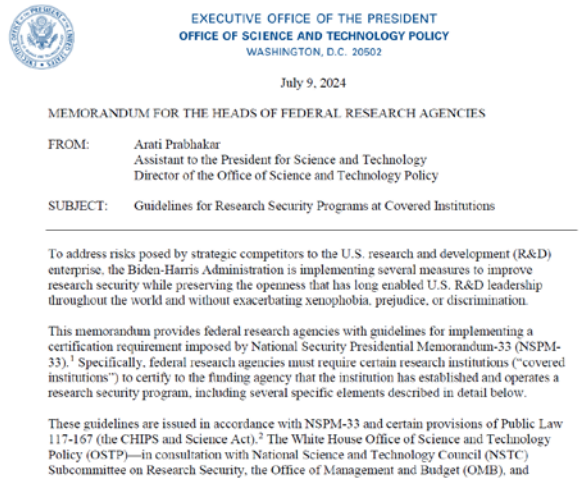
Department of Homeland Security (DHS) **Cybersecurity Readiness Factor**

- Applies when contractors will have access to CUI (as defined in the regulation).
- Contractors will submit a questionnaire and will be deemed to have: (1) a high likelihood of cybersecurity readiness; (2) a likelihood of cybersecurity readiness; or (3) a low likelihood of cybersecurity readiness.
- Even with a low likelihood of cybersecurity readiness, offeror will not be eliminated though may need to take care of controls after award.
- Graded against NIST SP 800-171 and SP 800-172.

Research Security Regulations – NSPM 33

Institutions receiving more than $50 in federal funding must implement a research security program (RSP), which includes measures to protect sensitive research data, manage foreign collaborations, and monitor potential conflicts of interest. Elements include:

1. **Cybersecurity** – program should be consistent with the National Institute of Standards and Technology (NIST)
2. **Foreign travel security** – should provide periodic training to those engaged in international travel and implement a travel reporting program
3. **Research security training** – has to be provided to all covered individuals
4. **Export control training** – ensure individuals working with export-controlled technologies complete export control training either by the U.S. Department of Commerce's Bureau of Industry and Security or other training on export control requirements, requirements, and processes for reviewing foreign sponsors, collaborators, and partnerships.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

July 9, 2024

MEMORANDUM FOR THE HEADS OF FEDERAL RESEARCH AGENCIES

FROM: Arati Prabhakar
Assistant to the President for Science and Technology
Director of the Office of Science and Technology Policy

SUBJECT: Guidelines for Research Security Programs at Covered Institutions

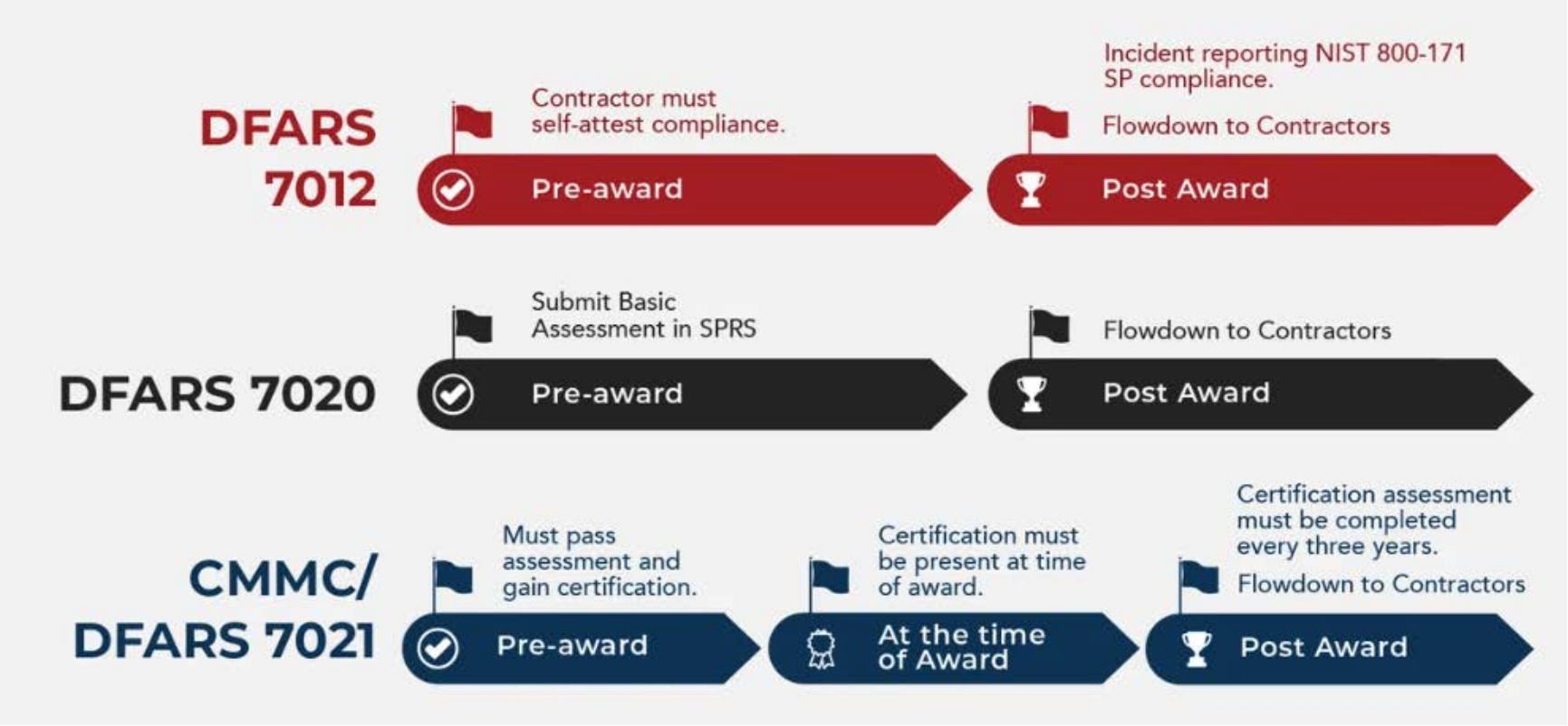
To address risks posed by strategic competitors to the U.S. research and development (R&D) enterprise, the Biden-Harris Administration is implementing several measures to improve research security while preserving the openness that has long enabled U.S. R&D leadership throughout the world and without exacerbating xenophobia, prejudice, or discrimination.

This memorandum provides federal research agencies with guidelines for implementing a certification requirement imposed by National Security Presidential Memorandum-33 (NSPM-33).[1] Specifically, federal research agencies must require certain research institutions ("covered institutions") to certify to the funding agency that the institution has established and operates a research security program, including several specific elements described in detail below.

These guidelines are issued in accordance with NSPM-33 and certain provisions of Public Law 117-167 (the CHIPS and Science Act).[2] The White House Office of Science and Technology Policy (OSTP)—in consultation with National Science and Technology Council (NSTC) Subcommittee on Research Security, the Office of Management and Budget (OMB), and

Defense Federal Acquisition Regulation Supplement (DFARS) Serie

252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting is the oldest of four clauses in the DFARS 70 Series (7012, 7019, 7020, and 7021)



DFARS 252.204-7012 (Update Forthcoming)

When it is Applicable: when the contractor has **Controlled Unclassified Information**. CUI is labeled by the Government OR is information of the type listed in the CUI Registry and is created or stored by the contractor in performance of the contract.

>100 categories in the CUI registry (http://www.archives.gov/cui/registry/category-list.html) which has expanded from roughly 30 in 2017. However, every company will have information that falls into at least four of the most common categories; privacy, procurement and acquisition, proprietary business information, and tax documents.

A company may also interact with CUI that falls into the **Export Control or Defense categories**

What it Requires:

- Compliance with 110 controls in NIST SP 800-171
- Notify DOD of incidents within 72 hours
- Cooperate with DOD in investigations
- This clause is currently being modified by the DAR Council
- As a baseline, every company must have a System Security Plan (SSP), and the SSP will need to address how the organization addresses all of the aforementioned requirements, the information systems within scope, and how the organization meets all requirements within DFARS 7012.

Which revision of NIST SP 800-171? Revision 2 (for now)

DFARS 7012 and CMMC overlap in several fundamental ways.

At the outset, CMMC requirements are established in DFARS via DFARS 7021; every Defense Industrial Base (DIB) supplier will have both requirements moving forward - especially after 2025. Also, the same flow down requirements are present in CMMC, and all subcontractors must follow similar requirements as the prime. Lastly, the most common thing shared among both regulations**, is the shared implementation of NIST 800-171. CMMC Level 2 includes all of NIST 800-171's 110 controls.**

CMMC Overview

CMMC 2.0 is a verification that contractors are complying with cybersecurity standards already in their contracts. **There are no new security controls required under CMMC.**

For contractors with Controlled Unclassified Information, CMMC will require (in almost all cases) a third-party verification by the Certified Third-Party Assessment Organization (C3PAO).

- The Level (and security controls) required will be determined by the contracting officer.
- Contractors that have not achieved a certification in the level required will not be awarded a contract.
- While CMMC will roll out over time, it is unknown which programs will be impacted first.
- Contracts solely for the provision of COTS products will be exempt from CMMC.

CMMC Overview

DoD Certifications Predictions

Level	Small	Other Than Small	Total
1 Self-Assessment	103,010	36,191	139,201
2 Self-Assessment	2,961	1,039	4,000
2 C3PAO Assessment	56,689	19,909	76,598
3 DIBCAC Assessment	1,327	160	1,487
Total	**163,987**	**57,299**	**221,286**

CMMC Overview

CMMC is implemented through two sets of rules:

CFR Part 32:
The CFR Part 32 Rule describes the CMMC program and set forth the “model” or the levels and the corresponding controls.
The CFR Part 32 Rule is final and effective December 16, 2024.
Actual CMMC assessments can begin as early as the effective date.

CFR Part 48:
The CFR Part 48 Rule implements the CMMC program into contracts.
The proposed version of the CFR Part 48 Rule was released in August 2024.
A final version of the CFR Part 48 Rule is expected to be effective in the first half of 2025.

CMMC Overview

CMMC Levels 1 and 2 already Map to Current Requirements:

Existing Requirement	Information Type	Controls	CMMC Mapping
FAR 52.204-21	Federal Contract Information	15 Controls in the FAR Clause	Level 1
DFARS 252.204-7012	Controlled Unclassified Information	110 Controls in NIST SP 800-171 (rev 2)	Level 2
None - NEW	Controlled Unclassified Information	24 Controls in NIST SP 800-172	Level 3

CMMC Overview

Expected Process

- A company that has Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) must self-assess or get a third-party assessment.
- The company establishes a scope for the assessment.
- The assessment covers the system defined from the scope.
- The system assessed is given a Unique Identification Number (UID).
- The contracting officer establishes the level needed in the solicitation and requires the assessed system UID upon award for the assessed system.

CMMC Overview

The Affirmation Process – All Levels 1-3

Who?

Affirmation must be completed by the "Affirming Official." The rule describes them as a "senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations." 170.22(a)(1)

What?

Affirmation must contain the following information: "Affirmation statement attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements to their CMMC Status for all information systems within the relevant CMMC Assessment Scope." 170(a)(2)(ii)

CMMC Overview

Time Line

- Original CMMC final interim rule (DFARS 252.204-21) referred to model with five levels all requiring third-party assessments.
- CMMC 2.0, announced in the Fall 2021, reduced five levels to three, eliminated DoD-specific requirements, and eliminated third-party assessments for level 1 (contractors handling federal contract information).
- On December 26, 2023, DoD released the new proposed CMMC programmatic rule and supporting documents.
- On August 15, 2024, DoD released the new proposed CMMC DFARS rule.
- In October 2024, DoD released the final programmatic rule.
- The final CMMC DFARS rule is expected Q1 2025.

CMMC Overview

Rapid Rollout: assumes March 1, 2025 final rule effective date:

Stage	Est. Timing	Required	Optional
1	March 1, 2025	• L1 and L2 Self-Assessments as condition of award.	• L1 and L2 Self-Assessment at option period for previously awarded contracts. • L2 C3PAO (Conditional) Assessments as condition for award.
2	March 1, 2026	• L2 C3PAO (Conditional) Assessments as condition of award.	• L3 DIBCAC (Conditional) Assessments as condition of award. • May delay L2 C3PAO (Conditional) Assessments until option period.
3	March 1, 2027	• L2 C3PAO (Conditional) Assessments for all option period for previously awarded contracts. • L3 DIBCAC (Conditional) Assessments as condition of award.	• May delay L3 DIBCAC (Conditional) Assessments until option period.
4	March 1, 2028	• All contracts and options will have the applicable CMMC requirements.	• None.

CMMC Overview

Expected Process

- A company that has Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) must self-assess or get a third-party assessment.
- The company establishes a scope for the assessment.
- The assessment covers the system defined from the scope.
- The system assessed is given a Unique Identification Number (UID).
- The contracting officer establishes the level needed in the solicitation and requires the assessed system UID upon award for the assessed system.

CMMI Overview

What CMMC 2.0 Means for Higher Education

Applicability: CMMC applies to universities and colleges, including research labs and facilities, federally funded research and development centers, and university-affiliated research centers. Certification may not apply to the entire institution — only to lab facilities conducting DoD-sponsored research.

Requirements: Depending on the type and sensitivity of the information being managed, universities and colleges handling Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) must achieve a particular CMMC certification level as a condition of the contract award.

Self-Assessment Option: Universities that process FCI and are seeking a maturity Level 1 certification will be allowed to conduct a self-assessment. The DoD may also permit universities seeking Level 2 certification to perform a self-assessment.

CMMI Overview

What CMMC 2.0 Means for Higher Education

Third-party Assessments: Universities that support critical national security programs and seeking Level 3 certification will have to get themselves assessed by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Certain Level 2 universities that work on CUI data may also be required to get an assessment done by CMMC Third-party Assessment Organizations (C3PAO).

Subcontractor Flow Down: If a university's domestic or international supply chain partner processes, stores, or transmits either CUI or FCI, then CMMC requirements will apply to them as well.

CMMI Overview

What Happens if Universities Fail to Demonstrate Compliance with CMMC?

The DoD has made it clear that if universities fail to meet CMMC requirements they will face major consequences. A university has not followed the stipulated cybersecurity practices, or has falsified its claims, then this could lead to loss of contracts and other penalties.

Non-compliant universities may be ineligible for future contract awards. The Department of Justice's Civil Cyber-Fraud initiative is already taking action against universities (e.g., Georgia Tech, Pennsylvania State University) that fail to meet the required cybersecurity standards.

CMMI Overview

What Happens if Universities Fail to Demonstrate Compliance with CMMC?

The DoD has made it clear that if universities fail to meet CMMC requirements they will face major consequences. A university has not followed the stipulated cybersecurity practices, or has falsified its claims, then this could lead to loss of contracts and other penalties.

Non-compliant universities may be ineligible for future contract awards. The Department of Justice's Civil Cyber-Fraud initiative is already taking action against universities (e.g., Georgia Tech, Pennsylvania State University) that fail to meet the required cybersecurity standards.

Approach

- Get Acquainted
- Determine the Scope
- Run A Gap Analysis
- Document Controls and Processes
- Conduct Self-Assessments Or Undergo A Formal Assessment

Approach

Get Acquainted: Understand the CMMC 2.0 requirements, as these may vary based on the DoD entity or the type of data you work with. For instance, universities engaged in highly sensitive research may be subject to more stringent requirements, while universities that rely on **commercial off-the-shelf (COTS) procurements** may be eligible for an exemption.

Determine the Scope: Identify all DoD research activities being performed. Gather information on all active DoD contracts. Identify external vendors that are managing sensitive data or information. Inventory all systems that are collecting, storing, or processing data related to DoD work.

Run A Gap Analysis: Assess your current cybersecurity controls and practices; compare them with the applicable CMMC requirements; identify any **gaps that exist** in the program; prioritize which areas you want to focus on first; and build a roadmap to achieve the desired compliance outcomes.

Approach

Document Controls and Processes: It's important to document and demonstrate your compliance against CMMC requirements. Ensure that all your controls, processes, and protocols for safeguarding information as well as procedures for responding and recovering from cybersecurity incidents are established and well-documented.

Conduct Self-Assessments Or Undergo A Formal Assessment: Depending on the level of CMMC certification your institution is seeking, you will be required to undergo a self-assessment or undertake a formal risk assessment using a government authorized C3PAO.

Agenda

- Introduction
- History and Background
- The Audit Perspective – Audit Approach
- Key Challenges
- Root Causes
- Conclusion
- Resources
- Q&A

Specificities of academic Institutions

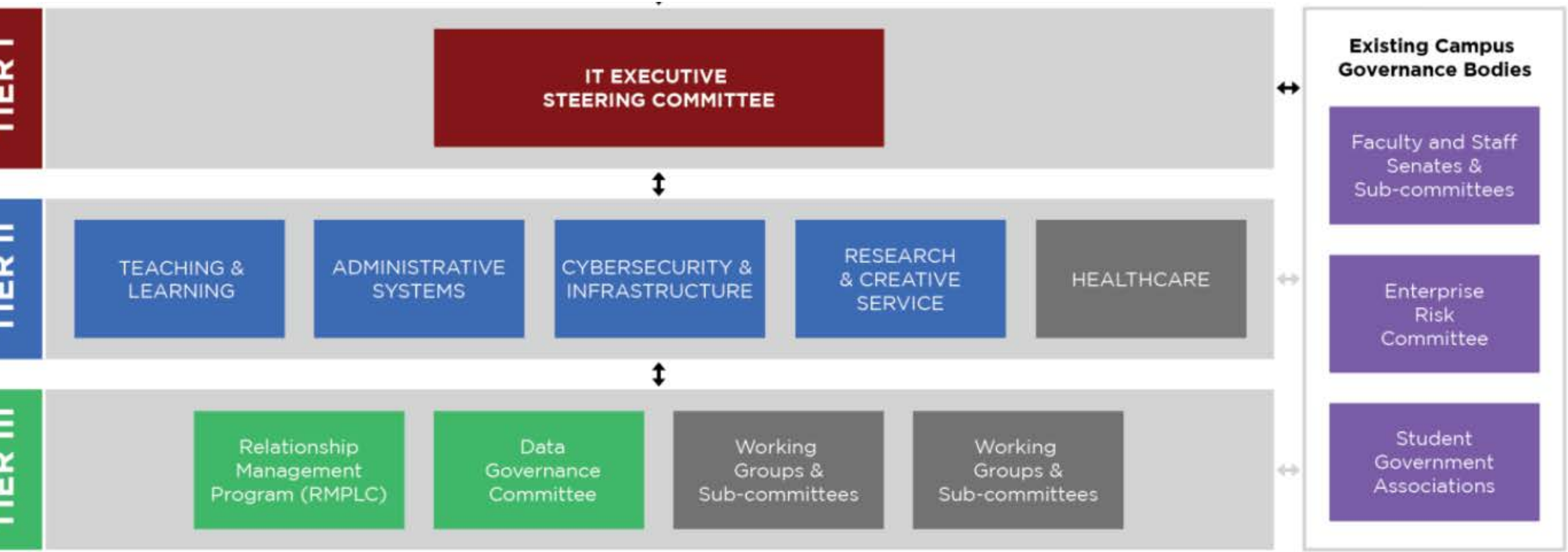
- Academic Freedom
- Many different cultures
- Focus on Opportunities
- Open Data
- Very different categories of data in the same environment (Health, Research, Admin,…)
- Decentralized Organization (Autonomy of the Faculty/Research Units)
- Departmental IT / Decentralized/Shadow IT
- IT Support providing by Academic Staff instead of centralized IT Support
- Data Exchange / Clouds
- Costs of Data Security impacts Research Budget
- Grants Compliance
- (Unsecure) Remote Access to Research and Administration Information from everywhere

IT Environment in Academic Institutions

- Diversified IT environment
- Decentralized IT / Shadow IT
- Legacy Systems
- Cost Allocation
- Cloud is getting common (application, infrastructure, services, etc.)
- Many regulatory requirements
- Constantly new and changing threats/risks related to the use of technology
- «Ownership» and «value» of information
- Immature IT/Information Security

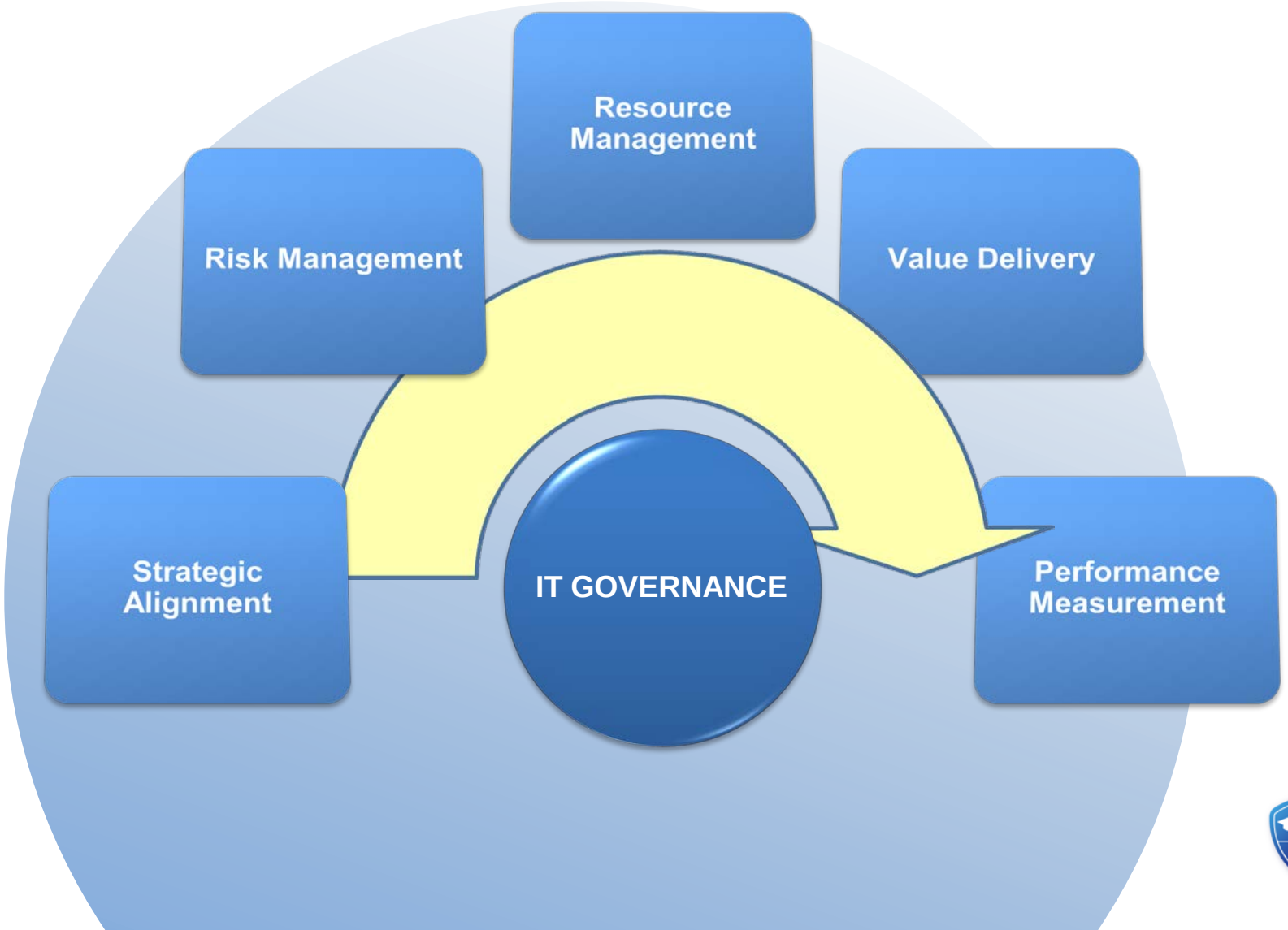
The Internal Audit Approach – What Create the Most Value?

- IA Risk Assessment – Research a key risk (positive/negative risks)
- IIA Requirements
- Research Program and Strategy
  - Strategy
  - Roles/responsibilities
  - Cybersecurity requirements (current and coming)
  - Other related requirements related to IT security …
  - IT Infrastructure
  - Cost
  - Measurements/metrics
  - IT and Information Governance
- Current Security Research Program
- CMMC program
- CMMC Gap Assessment


TIER I
IT EXECUTIVE STEERING COMMITTEE
TIER II
TEACHING & LEARNING
ADMINISTRATIVE SYSTEMS
CYBERSECURITY & INFRASTRUCTURE
RESEARCH & CREATIVE SERVICE
HEALTHCARE
TIER III
Relationship Management Program (RMPLC)
Data Governance Committee
Working Groups & Sub-committees
Working Groups & Sub-committees
Existing Campus Governance Bodies
Faculty and Staff Senates & Sub-committees
Enterprise Risk Committee
Student Government Associations

What is IT Governance?

Executive management and the board of directors are responsible for governing IT to add value and balance risk versus returns in IT.



Agenda

- Introduction
- History and Background
- The Audit Perspective – Audit Approach
- Key Challenges
- Root Causes
- Conclusion
- Resources
- Q&A

Level 1 17 Requirements – Cyber Hygiene

I. Domain – Access Control (AC)
– AC.1.001 – Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)
– AC.1.002 – Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
– AC.1.003 – Verify and control and/or limit connections to, and use of, external information systems.
– AC.1.004 – Control Information Posted or Processed on Publicly Accessible Information Systems

II. Domain – Identification and Authentication (IA)
– IA.1.076 – Identify Information System Users, Processes Acting on Behalf of Users and Devices
– IA.1.077 – Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems

III. Domain – Media Protection (MP)
– MP.1.118 – Sanitize or destroy information system media containing Federal contract information before disposal or release for reuse

IV. Domain – Physical Protection (PE)
– PE.1.131 – Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
– PE.1.132 – Escort Visitors and Monitor Visitor Activity
– PE.1.133 – Maintain Audit Logs of Physical Access
– PE.1.134 – Control and Manage Physical Access Devices

V. Domain – System and Communication Protections (SC)
– SC.1.175 – Monitor, control, and protect organizational communications (i.e., Information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of information systems.
– SC.1.176 – Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks

VI. Domain – System and Information Integrity (SI)
– SI.1.210 – Identify, Report and Correct Information and Information Flaws in a Timely Manner
– SI.1.211 – Provide protection from malicious code at appropriate locations within organizational information systems.
– SI.1.212 – Update Malicious Code Protection Mechanisms When New Releases are Available.
– SI.1.213 – Perform periodic scans of information systems and real-time scans of files from external sources as files are downloaded, opened or executed.

Level 2 Domains (110 controls)

- **Access Control (AC):** Focuses on limiting and monitoring access to critical information, including 22 specific controls.
- **Audit and Accountability (AU):** Ensures that actions within the system are tracked and can be reviewed, with 9 controls.
- **Awareness and Training (AT):** Provides training to all personnel on cybersecurity risks and procedures, with 3 controls.
- **Configuration Management (CM):** Manages the configuration of systems and software to maintain security, with 9 controls.
- **Identification and Authentication (IA):** Ensures that only authorized users can access systems and data, with 11 controls.
- **Incident Response (IR):** Defines procedures for responding to and recovering from security incidents, with 3 controls.

Level 2 Domains and Key Controls:

- **Maintenance (MA):** Ensures that systems and software are maintained in a secure state.
- **Media Protection (MP):** Protects sensitive information stored on removable media.
- **Personnel Security (PS):** Addresses security-related aspects of personnel, such as background checks and security awareness training.
- **Risk Assessment (RA):** Identifies and evaluates risks to information systems.
- **Security Assessment (CA):** Conducts regular security assessments to identify vulnerabilities.
- **System and Information Integrity (SI):** Maintains the integrity of systems and information.

Level 3 – Level 2 and 24 controls in the following domains:

- Access Control (AC)
- Awareness and Training
- Configuration Management
- Identification and Authentication
- Incident Response
- Personnel Security
- Risk Assessment
- Security Assessment
- System and Communication Protection
- System and Information Integrity

Key CMMC Challenges

Area	NISP SP 800-171
CUI Encryption	3.13.11
Multifactor Authentication	3.5.3
Flaw Remediation	3.14.1
Risk Assessment	3.11.2
Vulnerability Scan	3.11.1
Event Review	3.3.3
Audit Failure Alerting	3.3.4
Audit Correlation	3.3.5
System Baselining	3.3.5
Incident Response Testing	3.6.3

Key CMMC Challenges

1. Scoping
2. Program objectives and oversight
3. Documentation of the environment
4. Evidence of controls and process design
5. Supply Chain

Assessment

1. See Assessment guides provided by DoD
2. Policies/Standards
3. Procedures
4. Tools
5. Implementation
    1. All areas and layers
6. Governance
    1. Roles
    2. Measurements/Metrics
    3. Oversight

Agenda

- Introduction
- History and Background
- The Audit Perspective – Audit Approach
- Key Challenges
- Root Causes
- Conclusion
- Resources
- Q&A

Root Causes

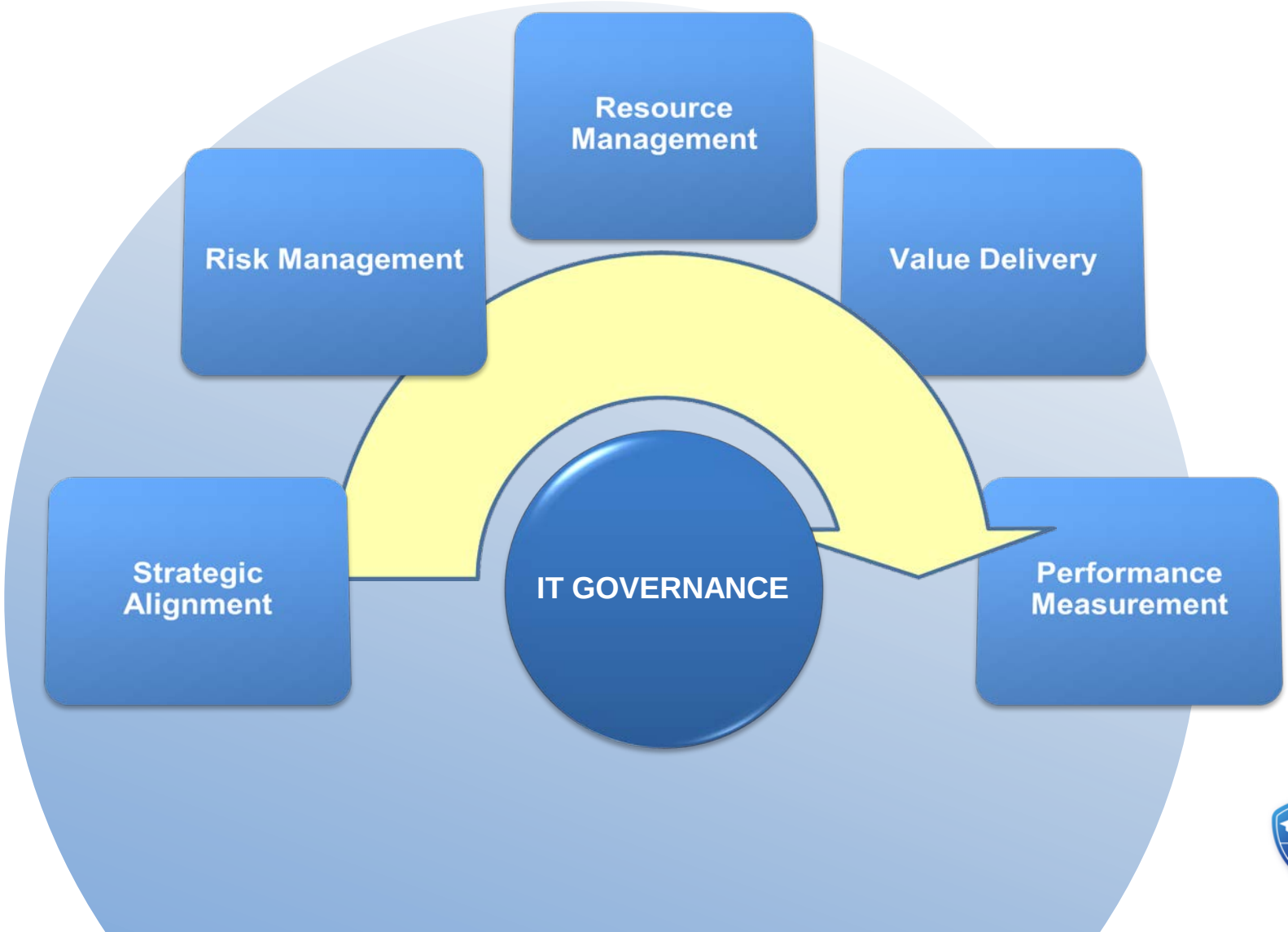
- Comprehensive Research Program and Strategy
- Research Security Program
- IT Governance
  - IT Strategy / IT enterprise architecture
  - Measurements/metrics
  - Value (understand investment/maintenance, TCO)
- Asset Management
  - Data
  - Software
  - Hardware
  - Data flow
  - Attributes
- Scoping

Root Causes (continued)

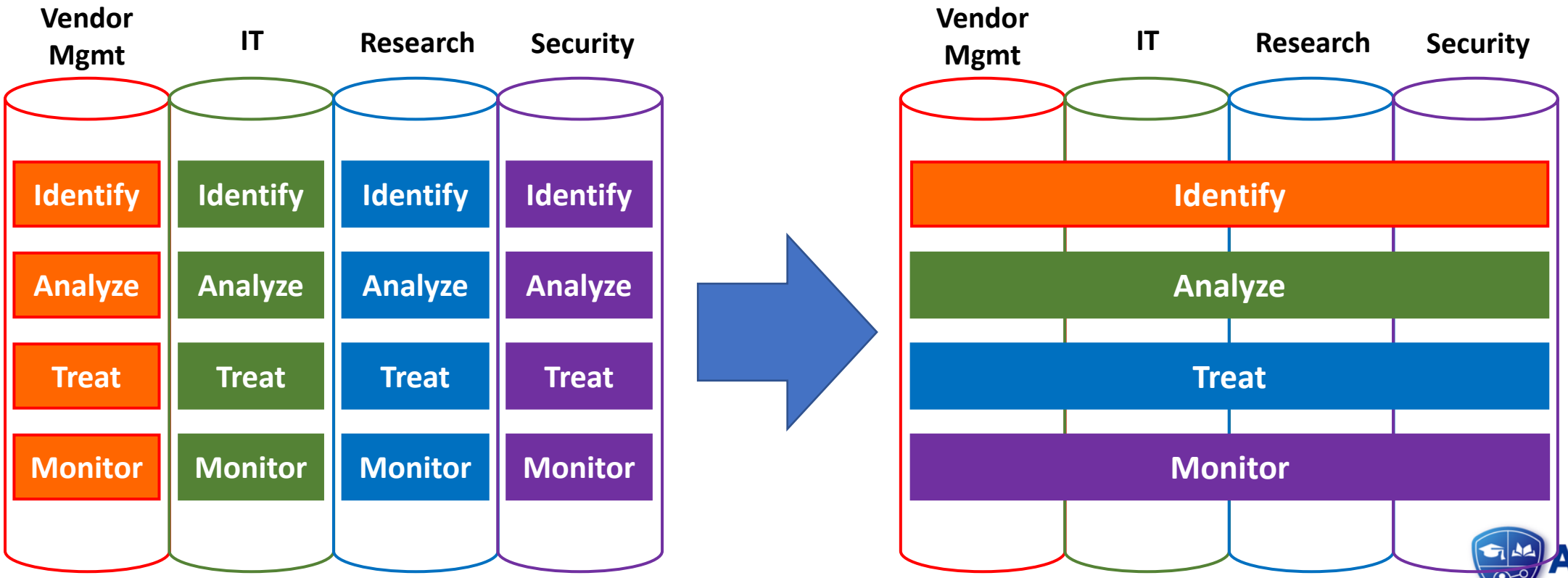
- Supply Chain Management
- Resources/Cost
- Silos
- Segmentation
- Procedures
- Evidence management and processes

What is IT Governance?

Executive management and the board of directors are responsible for governing IT to add value and balance risk versus returns in IT.



Silos


Vendor Mgmt
IT
Research
Security
Identify
Analyze
Treat
Monitor
Identify
Analyze
Treat
Monitor
Identify
Analyze
Treat
Monitor
Identify
Analyze
Treat
Monitor
Vendor Mgmt
IT
Research
Security
Identify
Analyze
Treat
Monitor

How to Address Root Causes

- Awareness
- Education
- Value
- ….
- Pain points

Source: COBIT 2019 Framework (© 2018 ISACA)

Agenda

- Introduction
- History and Background
- The Audit Perspective – Audit Approach
- Key Challenges
- Root Causes
- Conclusion
- Resources
- Q&A

Conclusion

- Focus on Internal Audit high value areas
- Not one approach to assesses CMMC
- What is coming … more requirements…
- Enterprise view
  - Risk management/ERM
  - IT Governance
  - Cost/TCO
  - Architecture
  - Objectives/measurements/metrics
  - Oversight
- Root Causes

Agenda

- Introduction
- History and Background
- The Audit Perspective – Audit Approach
- Key Challenges
- Root Causes
- Conclusion
- Resources
- Q&A

References

https://dodcio.defense.gov/cmmc/Resources-Documentation/

Q & A

Contact information

Johan Lidros

johan.lidros@emineregroup.com

+1 813) 832-6672 x-9101

+1 (813) 355-6104 (cell)

Ongoing IT Risk/Cybersecurity Updates

Interested in on-going IT Governance and IT Security updates? Sign up for our weekly newsletter “RiskIT “at https://www.emineregroup.com/subscribe/ or Linkedin Eminere Group Risk IT Newsletter