Attachment A

UCF

University Audit Update

February 26, 2025

Future Project Selection – Weighted Factors

Primary	Secondary	Tertiary
Mandatory requirement or requests by management, Board of Governors, or Board of Trustees	High visibility and reputational risk	First time audits or length of time since last audit
Impact on major university initiatives or strategic plan	Potential for consolidation and automation or cost savings opportunities	Potential for fraud risk
	Process and technology complexity; single point of failure; high degree of specialization or expertise	*Coordination with UCF's Enterprise Risk Management program
	Significant changes to regulations, programs, procedures, management, organizational structure, or employee turnover	

Other Considerations

- ❖ Timing and overall coverage; avoiding audit fatigue and coordinate with major initiatives and consulting engagements
- ❖ Audit work as an opportunity to provide UCF a competitive advantage
- ❖ Project scope and type (assurance vs advisory)
- ❖ Cost/benefit evaluation
- ❖ Available staffing and skill sets
- ❖ Begin with the end in mind—what will be different because of this audit project
- ❖ Ongoing risk assessment work which impacts project scores and future schedule

Upcoming Audits

Cycle 1	Cycle 2	Cycle 3
Financial Aid	College of Arts and Humanities	Performance-Based Funding
UCF Convocation Corporation (DSO)	UCF Global	TBD
TBD	TBD	TBD

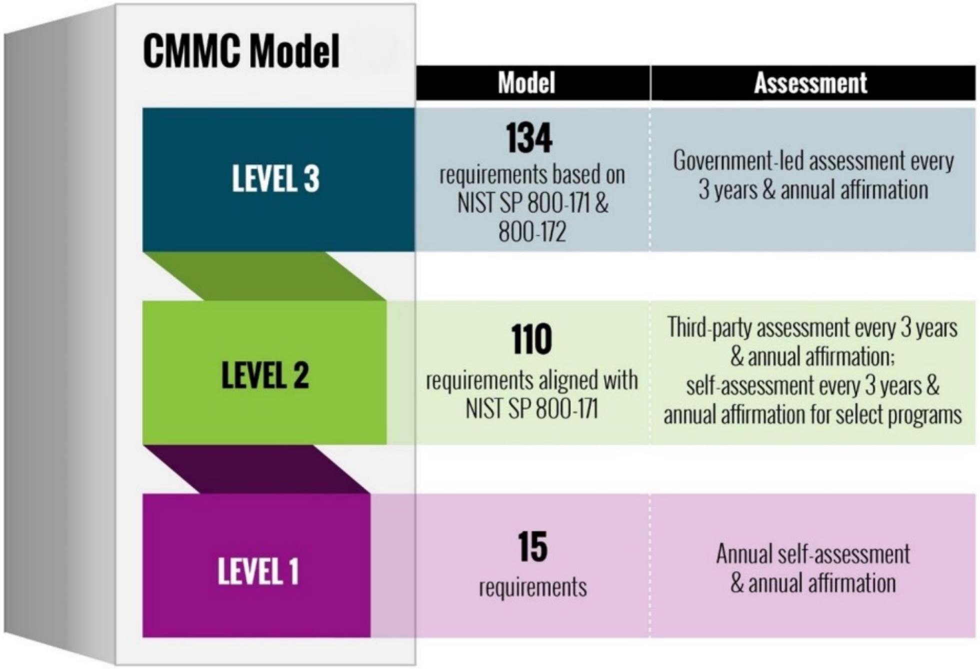
Watch List

- Undergraduate and/or Graduate Admissions
- Business Services
- Human Resources Benefits
- Academic Advising
- Direct Connect
- Stadium Construction Project

What is CMMC?

- **Cybersecurity Maturity Model Certification (CMMC)** is a Department of Defense (DoD) framework requiring institutions to safeguard **Controlled Unclassified Information (CUI)** to continue receiving federal research funding.
- **Mandatory for DoD Contracts** – Research institutions must meet specific security levels to conduct defense-related research.

CMMC Model Levels



CMMC Model

	Model	Assessment
LEVEL 3	**134** requirements based on NIST SP 800-171 & 800-172	Government-led assessment every 3 years & annual affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171	Third-party assessment every 3 years & annual affirmation; self-assessment every 3 years & annual affirmation for select programs
LEVEL 1	**15** requirements	Annual self-assessment & annual affirmation

Figure 1. CMMC Level Overview

The CMMC model consists of 14 domains that align with the families specified in National Institute of Standards & Technology (NIST) SP 800-171 Rev 2

Access Control	Media Protection
Awareness & Training	Personnel Security
Audit & Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification & Authentication	Security Assessment
Incident Response	System and Communication Protection
Maintenance	System and Information Integrity

Key Challenges for Research Universities

1️⃣ **Complex Research Environments** – Open collaboration models conflict with rigid security controls.

2️⃣ **Decentralized IT Infrastructure** – Multiple IT systems make standardization difficult. Need for customized documentation.

3️⃣ **Resource Constraints** – Significant costs in cybersecurity staff, training, and technology upgrades. Documentation resource challenges.

4️⃣ **Faculty Resistance** – Researchers may see security controls as disruptive.

5️⃣ **Third-Party Risks** – Use of external partners and cloud services complicates compliance.

How is EisnerAmper assisting?

Three project activities

1) Policy and Procedures Documentation Staff Augmentation

2) Cybersecurity Maturity Model Certification (CMMC): Level 1 Gap Assessment

3) Cybersecurity Maturity Model Certification (CMMC): Level 2 Readiness Assessment