Adapting to NIST CSF 2.0: Navigating Changes and Challenges in Higher Education

ACUA WEBINARS

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

ACUA SOCIAL NETWORKING

ACUA Virtual Learning Director
Wendee Shinsato, CPA, CIA
Assistant Vice Chancellor
California State University

ACUA Virtual Learning Volunteer
Virginia L. Kalil, CIA, CISA, CFE, CRISC
Executive Director/Chief Internal Auditor
University of South Florida

ACUA Virtual Learning Volunteer
Christiana Oppong, CIA, CCSA
Senior Auditor
Princeton University

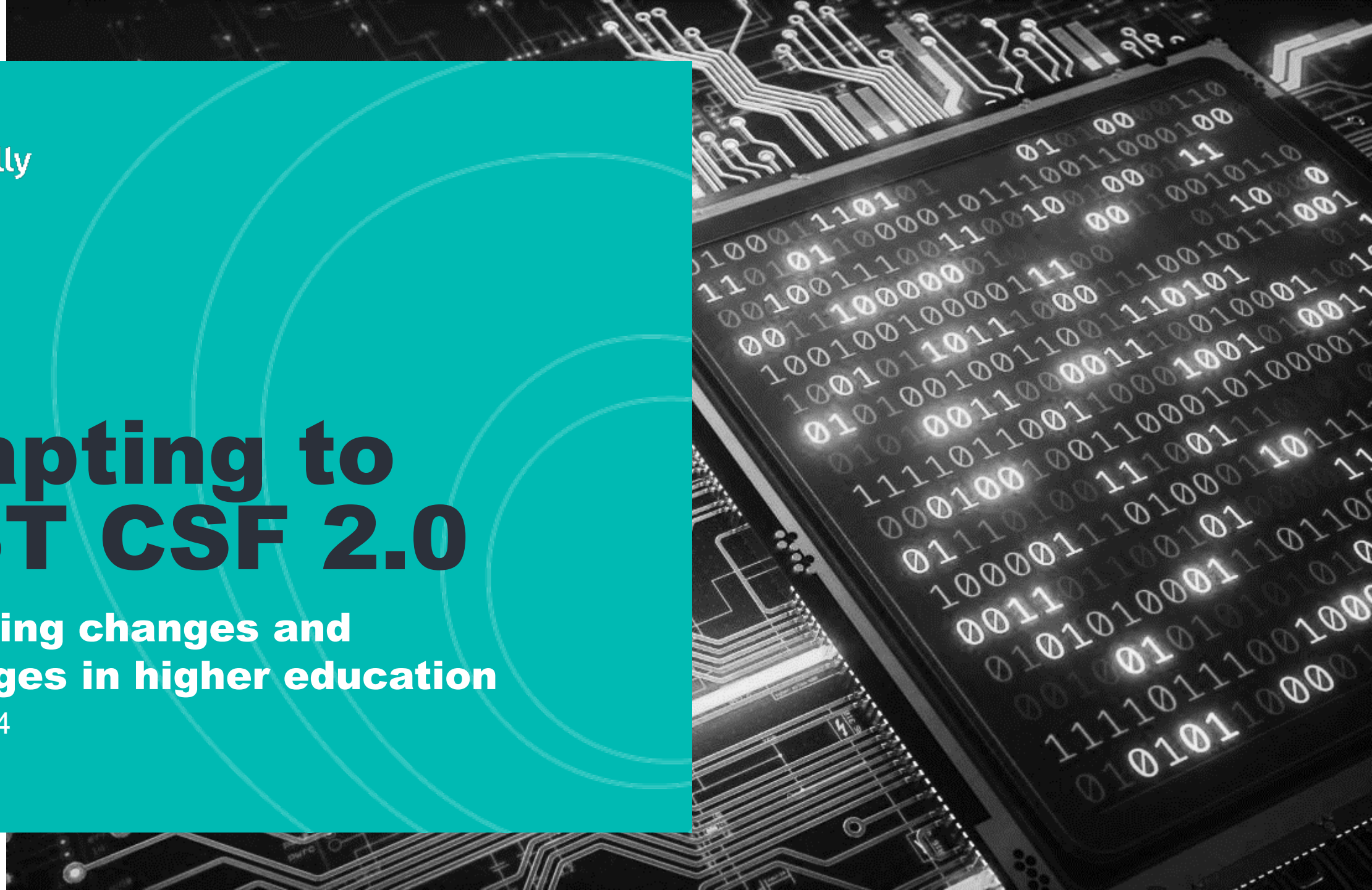
ACUA Virtual Learning Volunteer
Brenda Auner, CIA, CFE
Senior Auditor
California State University

bakertilly

Adapting to NIST CSF 2.0

Navigating changes and challenges in higher education

Oct. 17, 2024



Meet your presenters

Morgan Mincy, CPA, CISA

Manager, Risk Advisory | Baker Tilly

P: +1 (703) 923 8537
E: morgan.mincy@bakertilly.com

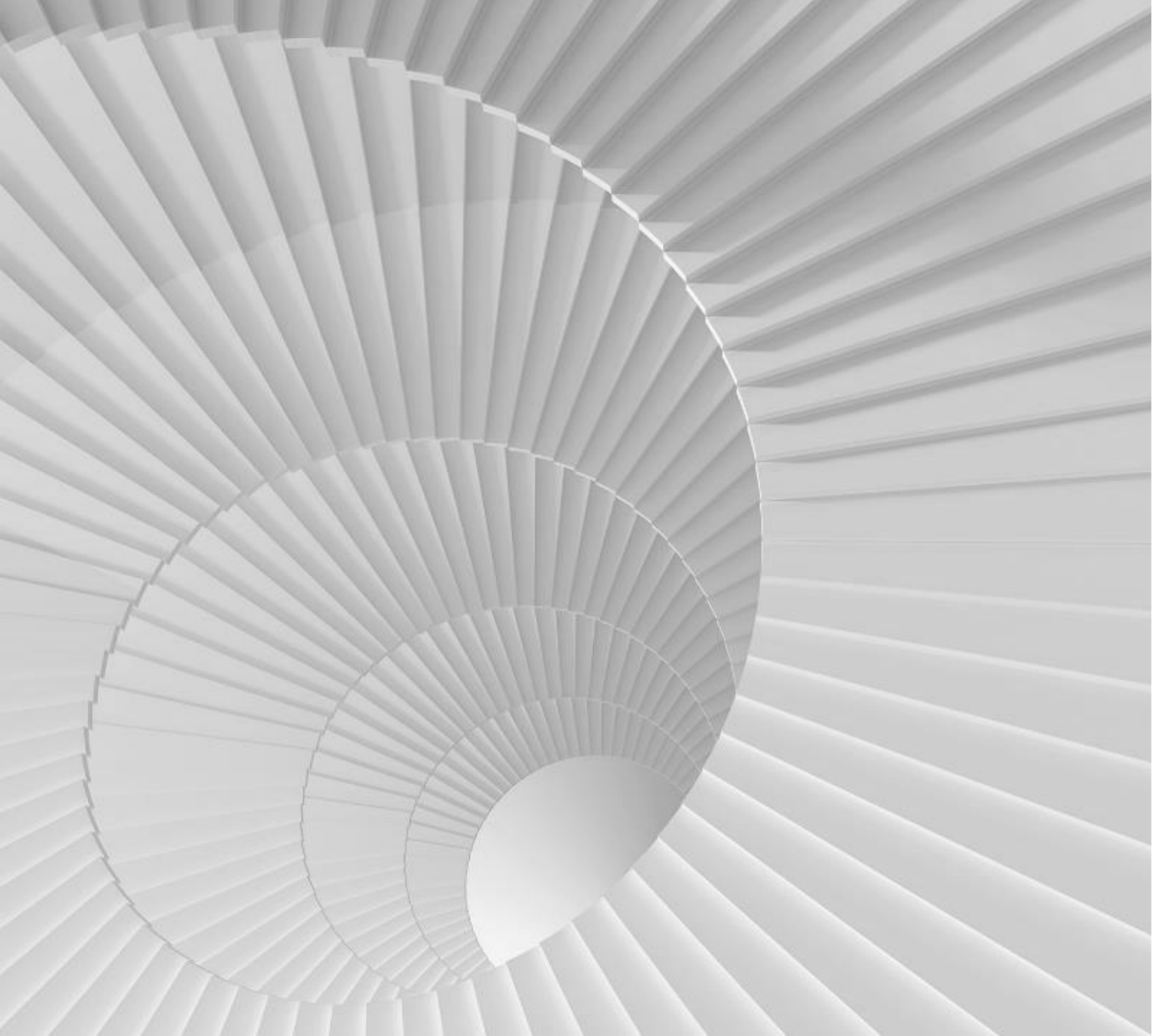
Amanda Vellocido, CPA, CISA

Manager, Risk Advisory | Baker Tilly

P: +1 (703) 827 3921
E: amanda.vellocido@bakertilly.com

Objectives

- Explore the challenges of implementing NIST CSF in higher education
- Understand the changes and impacts of the NIST CSF 2.0 version update
- Learn how institutions can conduct audits using the new version of NIST CSF



Polling question #1

Does your institution follow a specific cybersecurity framework or standard?

A) Yes

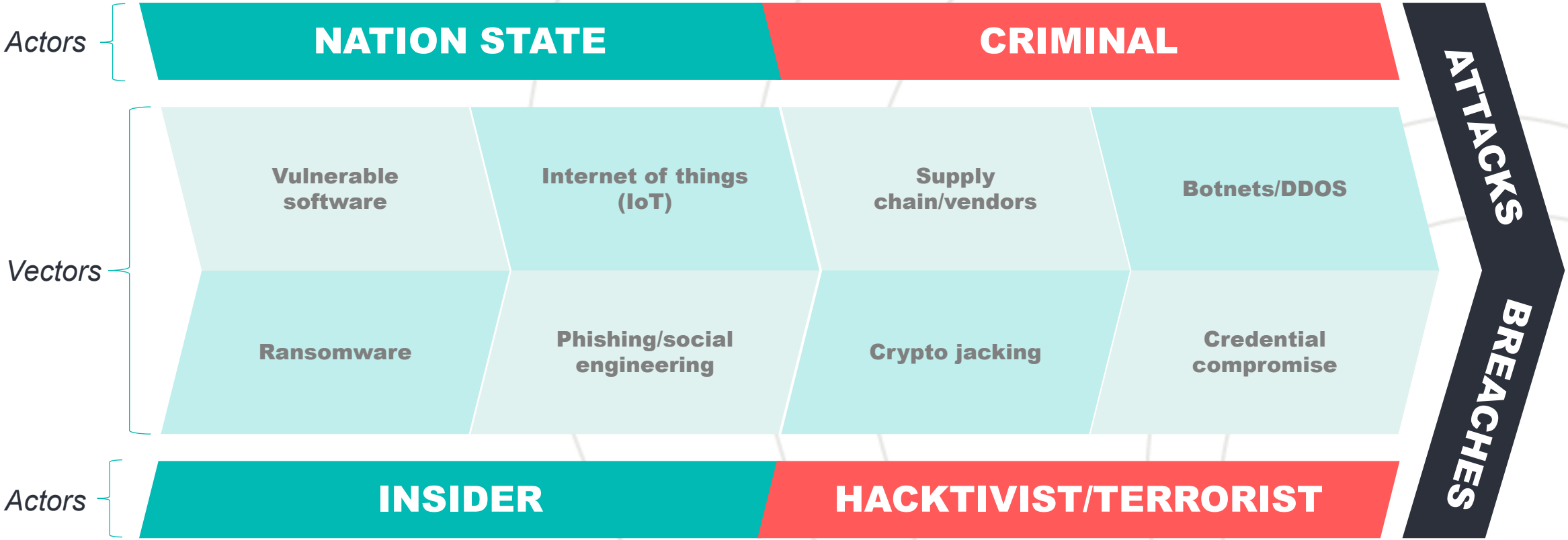
B) Sort of

C) No

D) Unsure

Cybersecurity threats and risks

Threats


Actors
NATION STATE
CRIMINAL
ATTACKS
BREACHES
Vectors
Vulnerable software
Internet of things (IoT)
Supply chain/vendors
Botnets/DDOS
Ransomware
Phishing/social engineering
Crypto jacking
Credential compromise
Actors
INSIDER
HACKTIVIST/TERRORIST

IT risks

Reputation	Competitive	Operational	Financial	Regulatory
Damage to brand/negative publicity	Loss of intellectual property	Loss of time spent to respond	Cost of response for incidents	Effort to address requirements
Damage to individual faculty/researcher professional standing	Damage to relationships with partners (e.g., research sponsors, other institutions)	Loss of ability to operate or continue work	Loss of future funding	Cost of fines, sanctions

Challenges within higher education

IT challenges

Distributed nature of IT systems, people and processes at universities

Limited and siloed authority for information security function

Size and complexity of IT environments

Various stakeholders responsible for cybersecurity activities

Culture values the open exchange of information for scholarship and research

Limited funding

Importance of using a framework

- Standardization and consistency
- Comprehensive coverage
- Regulatory compliance
- Credibility and trust
- Efficient use of resources
- Benchmarking

Changes and impacts of the NIST CSF 2.0 version update

Polling question #2

Has your institution evaluated the changes from NIST CSF 2.0 from NIST CSF 1.0?

A) Yes

B) Sort of

C) No

D) Unsure

What is NIST CSF?

Objectives

- Provide a structured, flexible framework that helps organizations understand, manage and mitigate their cybersecurity risk
- Promote risk management and the protection of data, systems and operations from cyber threats

Goals

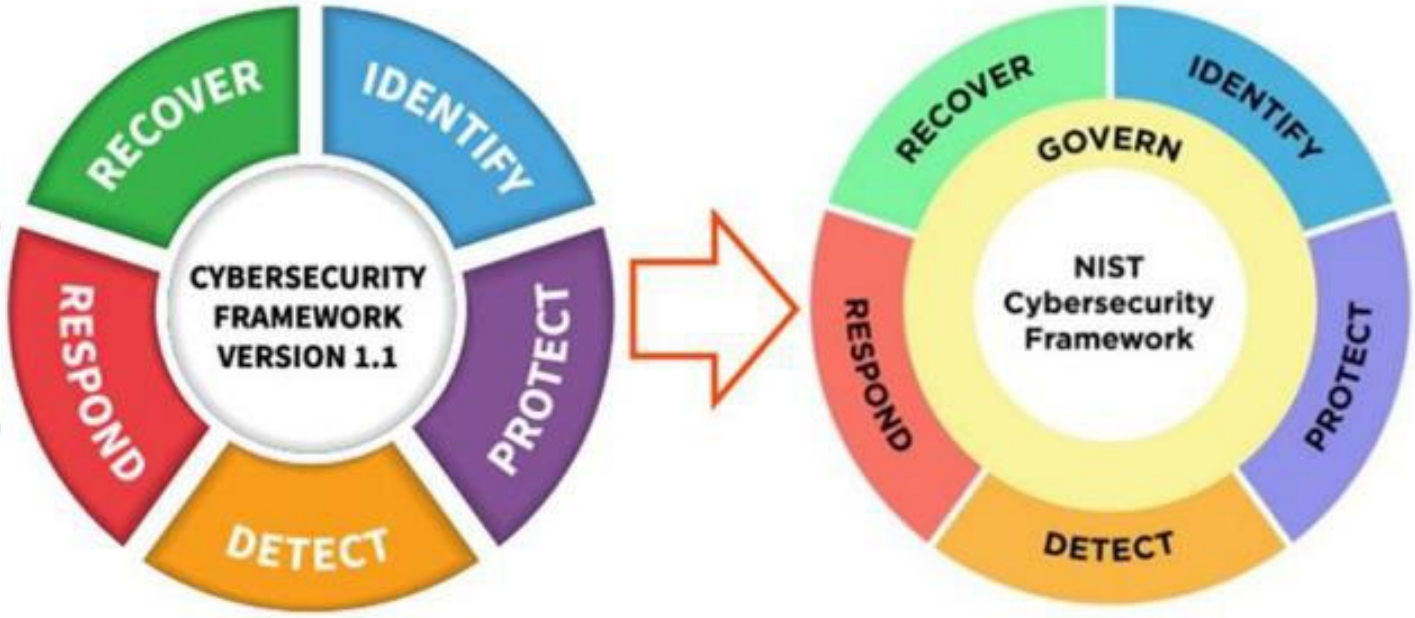
- Improve cybersecurity risk management
- Promote a common language
- Enhance resilience
- Flexibility and scalability

Importance

- Broad applicability
- Compliance and regulatory support
- Enhances communication
- Continuous improvement

NIST CSF 2.0 changes

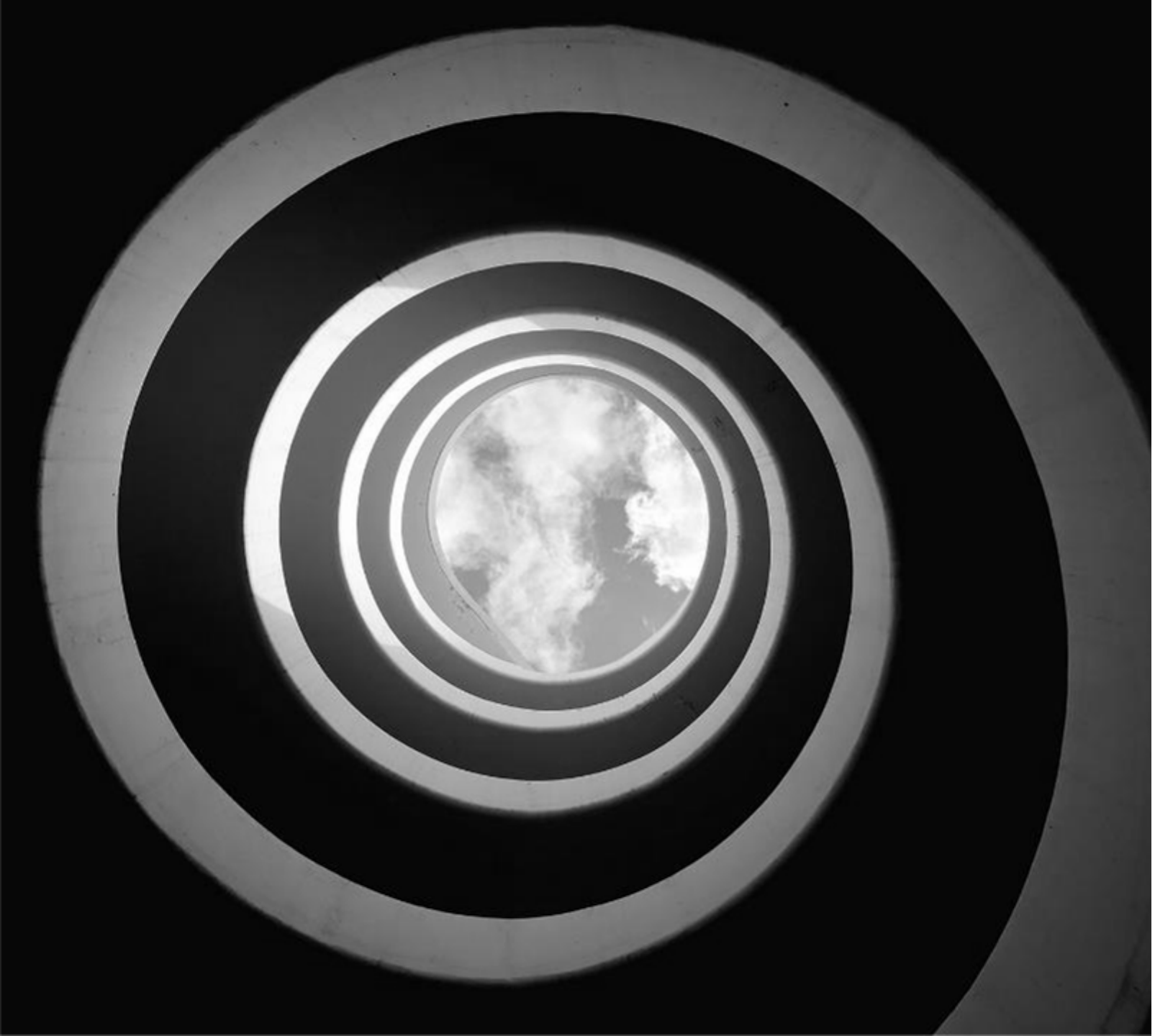
- Added a fifth function (i.e., domain) to address governance
- Added more details on cybersecurity supply chain risk management
- Added, clarified and reorganized the categories (e.g., groupings of protections) and subcategories (e.g., protections or controls)



Other NIST CSF changes

- ID.IM – Improvement
- PR.AA – Identity, management, authentication and access control
- PR.PS – Platform security
- PR.IR – Technology infrastructure resilience
- RS.MA – Incident management
- RC.RP – Incident recovery plan execution

Conducting audits with NIST CSF 2.0



Polling question #3

Has your institution conducted an audit using NIST CSF 2.0?

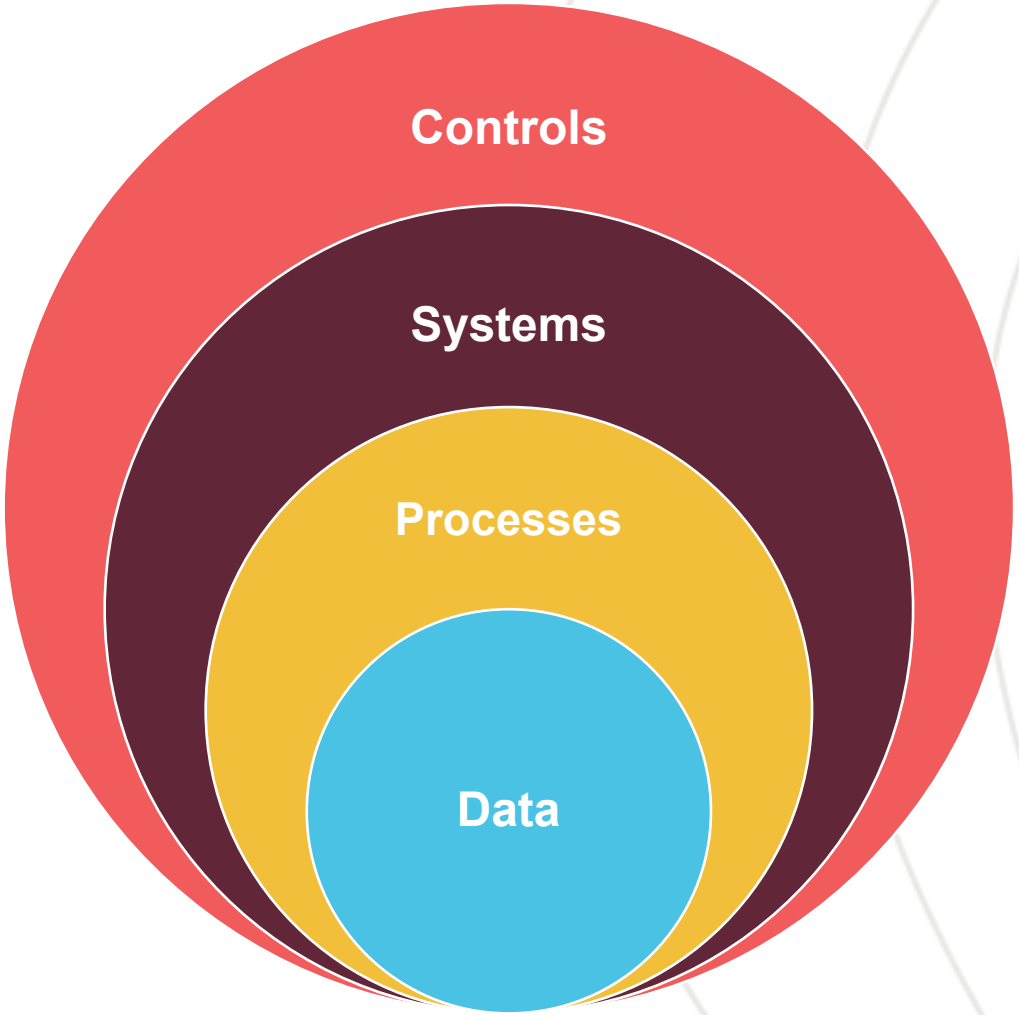
A) Yes

B) No, but we plan to

C) No

D) Unsure

Scoping



Examples

- NIST CSF
- Systems/applications
- User devices
- Infrastructure/network
- Asset management
- Access control
- Physical security
- PII
- CUI
- Export controlled
- ePHI

Approach

Enterprise wide

- Use NIST to evaluate controls owned at the enterprise level
- Combine with controls owned at the department level

Department approach

- Use NIST to evaluate controls owned at the department level
- Combine with controls owned at the enterprise level

Specific compliance

- Use NIST to evaluate specific requirements (e.g., GLBA)
- Evaluate the specific requirement across all applicable university systems

Polling question #4

Does your institution perform a mix of enterprise-wide, department specific and compliance specific audits?

A) Yes

B) No

C) Unsure

Now what?

- Gather relevant stakeholders
- Develop a roadmap
- Perform a NIST CSF 2.0 gap assessment
- Update cybersecurity safeguards based on identified gaps

Let’s recap!

Key takeaways

Identifying and implementing a recognized framework, such as NIST CSF 2.0, enables more effective and efficient audits

The NIST 2.0 updates will provide for the proactive adaption and continuous improvement of cybersecurity practices

Perform a gap assessment to jumpstart the implementation of NIST CSF 2.0 and to identify potential weaknesses in your institution’s cybersecurity posture

Questions? Connect with us.

Morgan Mincy, CPA, CISA

Manager, Risk Advisory | Baker Tilly

P: +1 (703) 923 8537
E: morgan.mincy@bakertilly.com

Amanda Vellocido, CPA, CISA

Manager, Risk Advisory | Baker Tilly

P: +1 (703) 827 3921
E: amanda.vellocido@bakertilly.com

bakertilly

Cybersecurity and IT risks

Video highlights

- **Types and example of IT risks higher education institutions encounter** such as reputational, competitive, operational, financial and regulatory issues
- **Recognized cybersecurity frameworks** commonly used by colleges and universities to standardize processes, ensure regulatory compliance and conduct more consistent, efficient audits
- **Best practices to** enhance an institution's risk management and cybersecurity posture, like the Institute of Internal Auditors' (IIA) Three Lines Model for effective governance and risk management
- Real examples of **cyber incident response and vulnerability management audits**

bakertilly.com/insights/cybersecurity-and-it-risks

Announcements

Upcoming ACUA Webinars

Month	Date & Time	Presenter	Topic
November	11/21/24 1:00pm EST	Workiva	Driving Change through Audit and Analytics
December	12/5/24 1:00pm EST	Baker Tilly	Compliance Hot Topics

New Kick Starter Available!

Assessing Voluntary University Climate Commitments

Download today in the members-only Audit Tools section of www.ACUA.org

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

Next Kick Starter Release is November 15th!

Information Technology – Third Party Risk Management

Will be available in the members-only Audit Tools section of www.ACUA.org

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

CONNECT WITH US

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

Working on a new audit subject? Looking for some best practices or insights from other higher education institutions? Connect with your colleagues on Connect ACUA! **Connect.ACUA.org**

Share your knowledge with others: Did you know that Connect ACUA allows you to post new messages directly from your email without logging in to the Connect ACUA website? Reply to a post today!

ACUA WEBINARS

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

Stay Updated

- The College and University Auditor is ACUA's official journal. Current and past issues are posted on the ACUA website.
- News relevant to Higher Ed internal audit is posted on the front page. Articles are also archived for your reference under the Resources/ACUA News.

Get Educated

- Take advantage of the several FREE webinars held throughout the year.
- Attend one of ACUA conferences:

Audit Interactive (Spring 2025)
AuditCon (Fall 2025)

- Contact ACUA Faculty for training needs.

Get Involved

- The latest Volunteer openings are posted on the front page of the website.
- Visit the listing of Committee Chairs to learn about the various areas where you might participate.
- Nominate one of your colleagues for an ACUA annual award.
- Submit a conference proposal.
- Present a webinar.
- Become a Mentor
- Write an article for the C&U Auditor.
- Write a Kick Starter.

Connect with Colleagues

- Subscribe to one or more Forums on the Connect ACUA to obtain feedback and share your insights on topics of concern to higher education internal auditors.
- Search the Membership Directory to connect with your peers.
- Share, Like, Tweet & Connect on social media.

Solve Problems

- Discounts and special offers from ACUA's Strategic Partners
- Kick Starters
- Risk Dictionary
- Mentorship Program
- NCAA Guides
- Resource Library
- Internal Audit Awareness Tools
- Governmental Affairs Updates
- Survey Results
- Career Center.....and much more.

ACUA WEBINARS

Join us for our upcoming webinar.