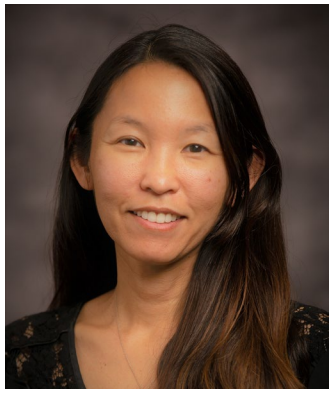
NSPM-33 and you: What it is and how to prepare and protect your institution

ACUA WEBINARS

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

ACUA SOCIAL NETWORKING



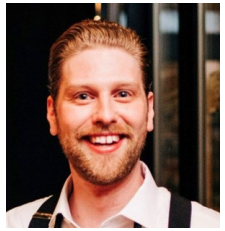
ACUA Virtual Learning Director
Wendee Shinsato, CPA, CIA
Assistant Vice Chancellor
California State University

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

Your Deloitte & Touche LLP facilitator team for today



Dillon Clark

Professional Background:

Dillon is an advisory manager and Certified Fraud Examiner (CFE) at Deloitte with more than 10 years of operational redesign, process development and implementation, non-profit and fund accounting, and organizational transformation experience. Dillon advises state, local government, and higher education clients through complex fund accounting and research compliance questions including system implementations and serves as a subject matter specialist for research administration and compliance to Internal Audit teams in Health Care and Higher Education.

Dillon previously served in multiple accounting, operations, and finance roles in the social and neuroscience research sectors. Most recently he served as the Director of Finance and Operations for an academic research firm where he oversaw the full GL cycle and operational growth management by designing and implementing systems, policies, procedures. He also managed multiple government and private philanthropic grants with expenditures in over five currencies and programmatic activities in three continents.

Elizabeth Walton

Professional Background:

Elizabeth is a senior manager with a primary focus in internal audit transformation and IT Internal Audit in the non-profit and higher education industries. She has focused on the design and development of Internal Audit programs as well as identifying, testing and designing internal controls to address key IT risks. Elizabeth has assisted with multiple IT risk assessments in the non-profit sector to categorize processes requiring greater review and control enhancement. Elizabeth has led the execution of internal audits in key IT risk areas in higher education such as 'Bring Your Own Device,' 'Data Lifecycle Management' and 'Cyber Security'. She has worked closely with universities to help them identify emerging risks and provided advisory services to develop controls and processes to mitigate the complex technology risks of the non-profit sector and higher education industry. Elizabeth currently serves as the lead Internal Audit Senior Manager for a top research institution and the Lead IT Internal Audit Manager for a large private university. In this role, Elizabeth has worked closely with the university to assess their risks, processes and controls in IT including their management of key systems.

Agenda

1. History
2. Framework
3. What are the Requirements?
4. Risks and Considerations

Objectives

1

Understand the history and scope of NSPM – 33

2

Articulate standards required for NSPM-33 Compliance

3

Understand the importance of monitoring and oversight of the controls required by NSPM-33

Polling Question: What is your familiarity with NSPM-33?

1. I have never heard of NSPM-33
2. I am somewhat familiar with NSPM-33
3. I am very familiar with NSPM-33
4. I am very familiar with NSPM-33 and my team is already taking steps to prepare for coming regulations

ACUA WEBINARS

TOPIC

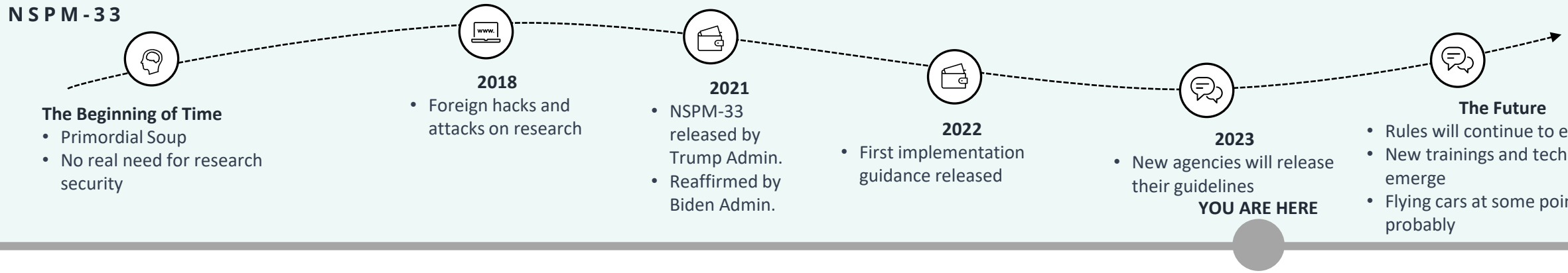
What is NSPM-33?

The Requirements

What is Internal Audit's Role

What is NSPM-33?

History

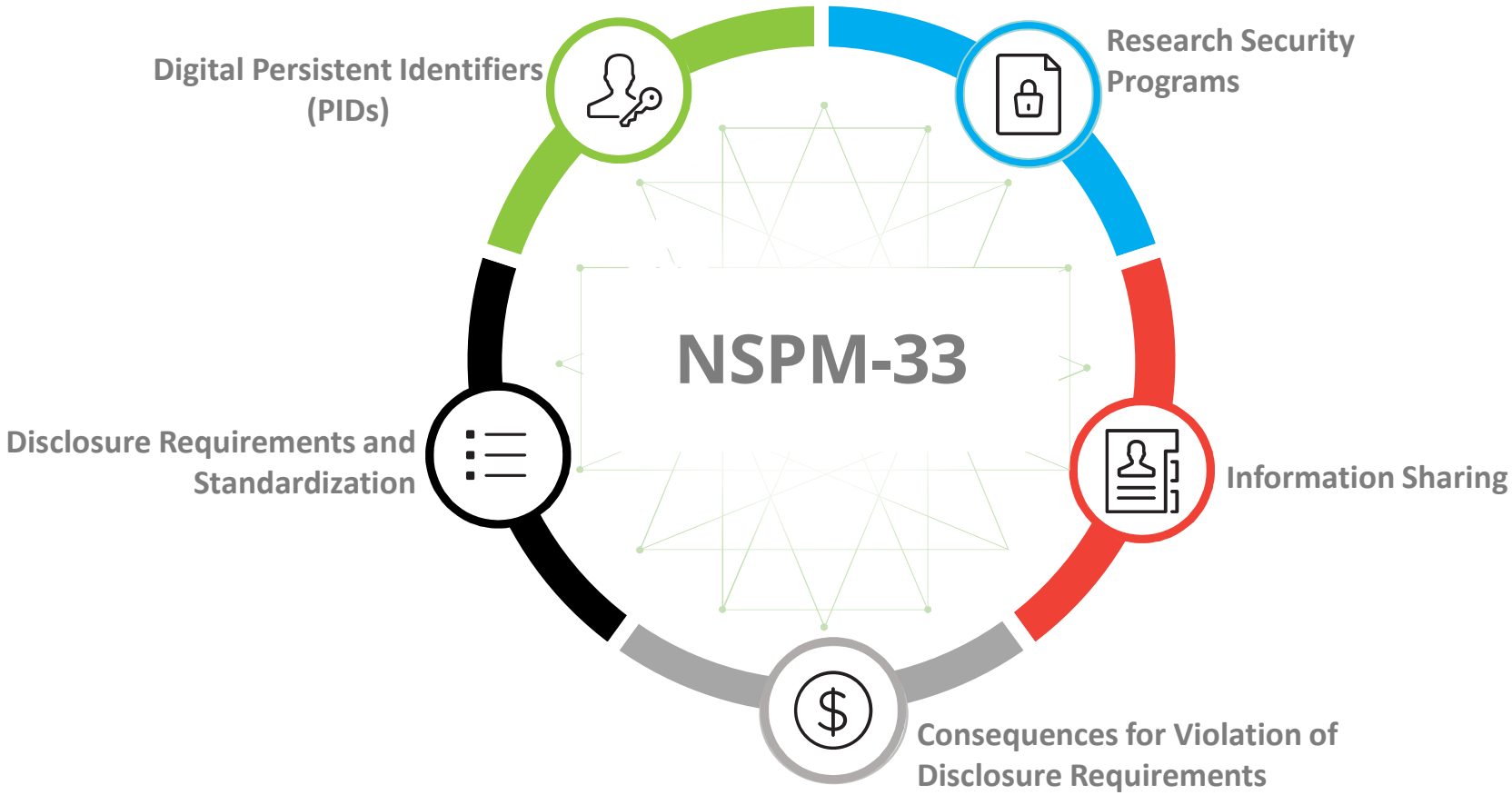

NSPM-33
The Beginning of Time
• Primordial Soup
• No real need for research security
2018
• Foreign hacks and attacks on research
2021
• NSPM-33 released by Trump Admin.
• Reaffirmed by Biden Admin.
2022
• First implementation guidance released
2023
• New agencies will release their guidelines
YOU ARE HERE
The Future
• Rules will continue to evolve
• New trainings and tech needs emerge
• Flying cars at some point, probably

What is NSPM-33: NSPM-33 is a Presidential Memorandum that provides directives to federal research funding agencies to strengthen and standardize controls to protect 'United States Government-support Research and Development (R&D) against foreign government interference and exploitation. The directive includes guidance on disclosure requirement standardization and security program development.

Why was NSPM-33 Issued: There has been an increasing need to protect US Research and Development from foreign governments while not overburdening researchers and limiting research advancement.

How does NSPM-33 Impact Higher Education: As recipients of federal R&D funds, institutions will need to respond to the updated disclosure requirements from federal research funding agencies. Additionally, the NSPM-33 implementation guidance released by the 'National Science and Technology Council' includes direct guidance for recipients of federal funds, including institutions of higher education, including the strengthening of security programs.

Overview of Elements



Polling Question: Have you performed a research related internal audit in the past 3 years?

1. Yes
2. No
3. Not Yet – but it's on our workplan
4. N/A – my institution does not perform research

The Requirements – A Deeper Dive

ACUA WEBINARS

PIDS

PIDs (also known as digital persistent identifiers)

What are they?

- A PID is a long-lasting reference to a digital resource. Unlike URLs, which may break, a *persistent* identifier reliably points to a digital entity.
- Like a journal article or book's DOI, but for a person

What are the requirements?

- Researchers must maintain required disclosure information in a "profile" or "Record"
    - Many researchers and institutions currently use ORCID* for creation of a unique number
- During the grant application process, researchers provide their PID and authorize the research agency to access their information

What are the benefits?

- PIDs allow researchers to maintain unique a number rather than using a common name
- Reduces administrative burden
- Allows greater understanding of researcher networks and awards
- Reduces duplicative efforts to update information

**ORCID is an international, interdisciplinary, open, non-proprietary, and not-for-profit organization created by the research community for the benefit of all stakeholders, including you and the organizations that support the research ecosystem. ORCID's name was formed from the acronym Open Researcher and Contributor Identifier*
https://support.orcid.org/hc/en-us/articles/360006973993-What-is-ORCID-#:~:text=ORCID's%20name%20was%20formed%20from,time%2C%20disciplines%2C%20and%20borders.

ACUA WEBINARS

Incorporating PIDS into grants, cooperative agreements and disclosures

1

Researcher maintains their individual profile with information required across agency disclosures. This profile is maintained by a PID service and is associated with a unique PID

2

During the grant application process, the individual provides their PID, the PID service, authenticates the PID and allows the research agency to see the required information. The researcher no longer has to input this information manually

3

The researcher certifies to the research agency that their PID is accurate and up-to-date.

4

The impact of variations between research agencies' application processes on the researcher will be reduced. The agency will have access to the PID containing the needed disclosure information

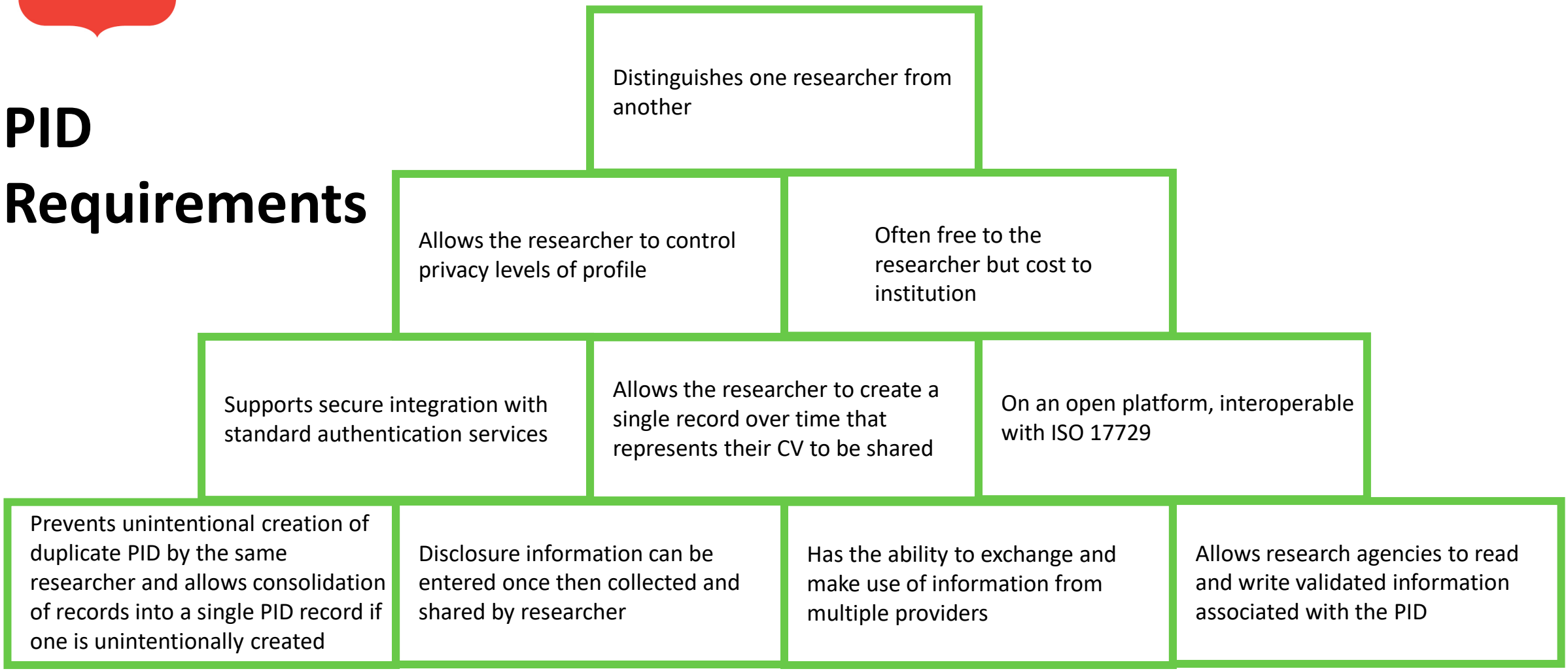
5

When research agency requirements exceed the standardized requirements, researchers can also maintain the additional disclosure information on their PID

6

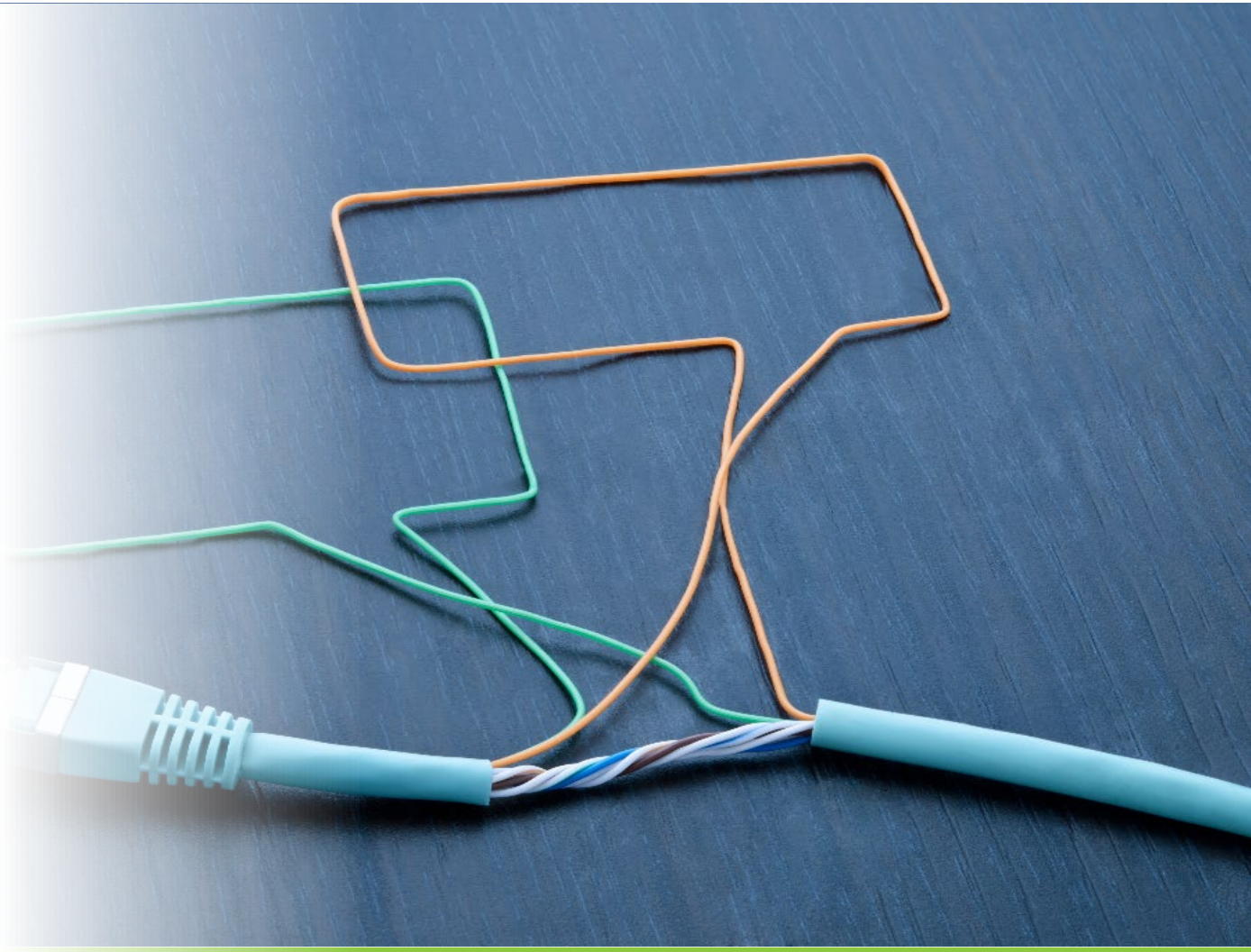
When annual or other updates are required, the researcher can easily provide an updated access allowance and certification their PID is still accurate and complete

PID Requirements



Information Sharing

“Research Agencies should share information about violations of disclosure requirements, consistent with due process, privacy considerations, and all other applicable laws”



https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

Disclosure Requirements

Where Disclosure Was

The research community is divided about disclosures. There have been cases in the past where researchers were wrongfully prosecuted due to the misunderstanding of a relationship.

Where Disclosure is Going

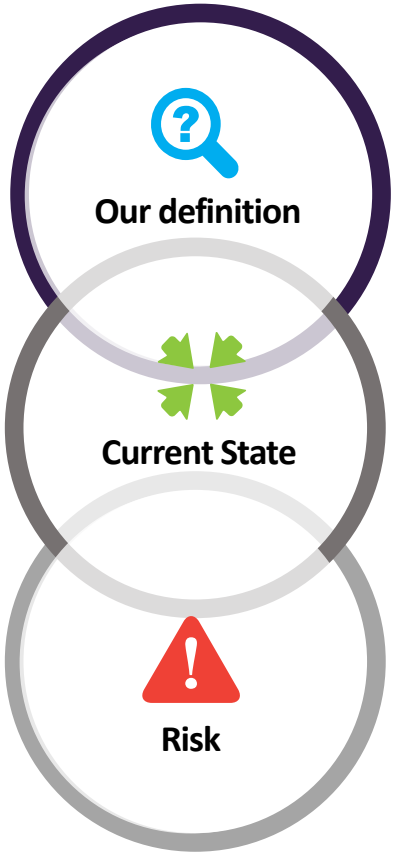
- Disclosure of foreign and other relationships required. Templates to be developed by funding agencies.
- A process for assessing high risk relationships may need to be created as well
  - PID can be useful in this area to allow for each researcher to have a unique identifier and remove ambiguity around relationships

Disclosures are going to become more common

Individual requirements will vary from agency to agency, but the federal government seeks to bring standardization

Disclosures Required From	Organizational Affiliations/ Employment	Positions/ Appointments	Foreign government-sponsored talent programs	Other Support
Tier I : Principal investigators (PIs) and other senior/key personnel, program officers, Intramural researchers	Y	Y	Y	Y
Tier II: Peer reviewers, advisory committee/Panel members	Y	Y	Y	N

Conflict of Interest



A situation in which an individual, or the individual's spouse or dependent children, has an interest or relationship (financial or otherwise) that could directly and significantly affect the design, conduct, reporting, or funding of research

Many universities already have disclosure requirements

Each funding agency can create their own policy

Some funding agencies are creating risk profiles and making funding decisions based on these profiles

Awards from conflicting agencies and governments put the quality of research at risk

Funding agencies may choose to not award funds to certain researchers or institutions of they determine that the risk profile is too high

Violations chip away at the integrity of research

DARPA Risk Portfolio Rubric

Rating	Factor 1: Foreign Talent Program	Factor 2: Denied Entity Lists	Factor 3: Funding Sources	Factor 4: Foreign Institutions or Entities
Very High	Indicators of active (ongoing) participation in a Foreign Talent Program run by the government of a strategic competitor or country with a history of targeting US technologies (CWHTUST) for unauthorized transfer.	Indicators of an active (ongoing) affiliation with an entity on the US Government identified denied entity or person list or EO 13959 or subsequent similar issuances.	Indicators of active (ongoing) direct funding from a foreign government or a foreign government-connected entity of a strategic competitor or CWHTUST.	Indicators of active (ongoing) affiliation with a high-risk foreign government, or foreign government-connected, institution or entity.
High	Indicators of past participation in a Foreign Talent Program run by the government of a strategic competitor or CWHTUST but with indications that a professional association with the program has continued.	Indicators of past affiliation or multiple recent associations (within the last four years) with an entity on the US Government identified denied entity or person list or EO 13959 or subsequent similar issuances.	Indicators of history/pattern of direct funding from a foreign government or from a foreign government-connected entity of a strategic competitor or CWHTUST.	Indicators of multiple active (ongoing) direct associations with a high-risk foreign government, or foreign government-connected, institution or entity.
Moderate	Indicators of active (ongoing) participation in a Foreign Talent Program run by the government of a U.S. ally who has technology sharing agreement with a CWHTUST.	Indicators of multiple past associations4 with an entity identified in the US Government denied entity list or EO 13959 or subsequent similar issuances.	Indicators of past non-consecutive, sporadic funding from a foreign government or foreign government-connected entity of a strategic competitor or CWHTUST	Indicators of multiple past direct associations with a high-risk foreign government, or foreign government-connected, institution or entity.
Low	No Participation in a Foreign Talent Program.	No Indicators of past or current association or affiliation with an entity on the US Government identified denied entity or person list or EO 13959 or subsequent similar issuances...	No indicators of past funding from a foreign government or foreign government-connected entity of a strategic competitor or CWHTUST.	No indicators of an association or affiliation with a high-risk foreign government, or foreign government connected, institution or entity.

Source: https://www.darpa.mil/attachments/092021DARPACFIPRubric.pdf

Polling Question: If you had a snow day tomorrow, how would you spend it?

1. Playing outside in the snow
2. Drinking Hot Cocoa while watching the snow inside my warm house
3. Binge watching my favorite shows
4. Checking a few things off my to-do list

$ Penalties

Implementation Guidance

- Agencies are expected to create “appropriate and effective consequences”
  - Up to, and including, debarment of eligibility for federal funding on top of potential criminal charges
- Depending on the facts surrounding the violation, funding agencies may pursue the following actions:
  - Rejection of an R&D award application;
  - Preserving an R&D award, but requiring or otherwise ensuring that individual(s) do not perform work under the award;
  - Ineligibility for participation in US Government review panels and other activities;
  - Suspension or termination of Federal employment;
  - Suspension or termination of an R&D award;
  - Suspension or denial of Title IV funds by the Department of Education; and
  - Placement of the individual or research organization in the System for Award Management or Federal Awardee Performance and Integrity Information System to alert other agencies.

Research Security Programs

Research Security Programs

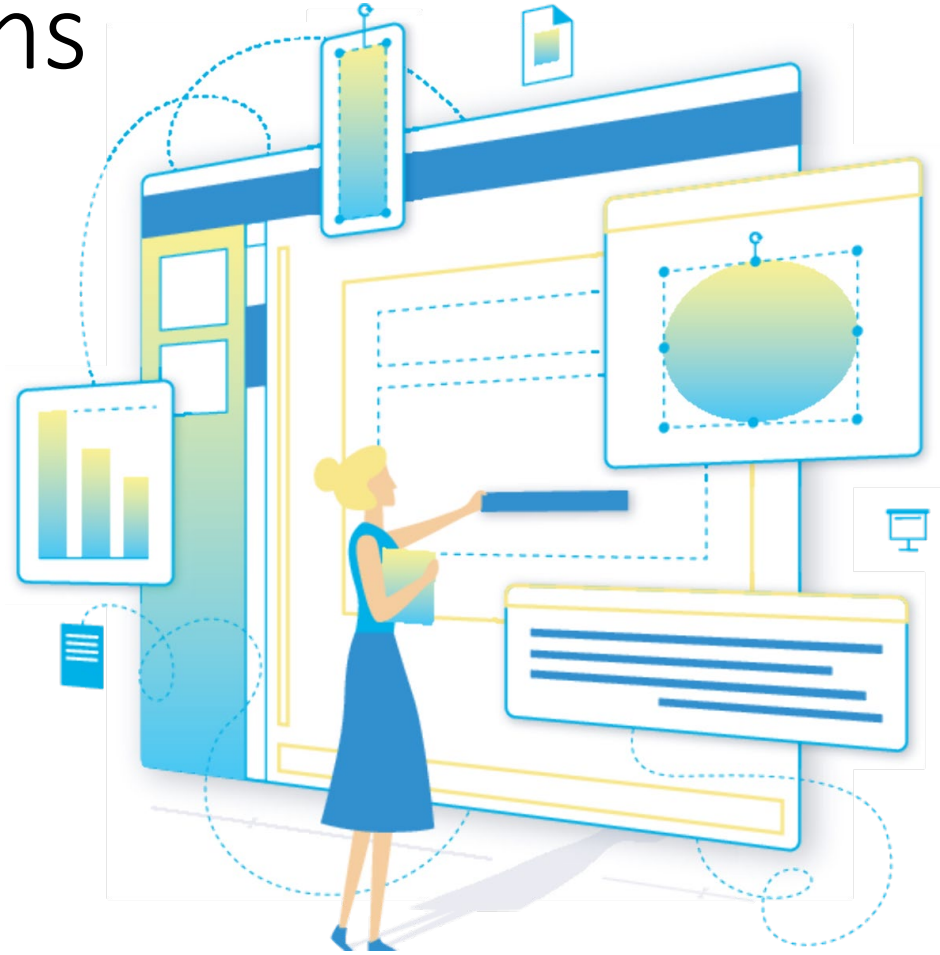
Section 4(g) of NSPM-33 directs that by January 14, 2022, “heads of funding agencies shall require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program…Heads of funding agencies shall consider whether additional research security program requirements are appropriate for institutions receiving Federal funding for R&D in critical and emerging technology areas with implications for United States national and economic security.”

https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

Research Security Programs

Made of four components:

- Cybersecurity
- Foreign Travel Security
- Research Security Training
- Export Control Training



Cybersecurity

Cyber is evolving into a distinct functional area of the business, transcending its traditional IT roots and becoming an essential part of the framework for delivering business outcomes.

Why is it relevant to Research

The world is increasingly interconnected, bringing about new risks alongside new growth opportunities. Digital technologies, exponential growth of data, and evolving business and research needs are expanding attack threat surfaces and bringing new challenges that elevate cyber as a strategic business issue.

What are the NSPM-33 requirements?

Research institutions that receive more than $50 million must establish and operate a research security program which should include a cyber security program. This Cyber program should include the elements we will highlight on the following slide.

What are the benefits?

Reduction in risk: Institutions are continuously targeted by internal and external sources. Effective cyber controls can help mitigate risk.

ACUA WEBINARS

NSPM-33's 14 Cybersecurity Elements

1. **Provide regular cybersecurity awareness training** for authorized users of information systems, including in recognizing and responding to social engineering threats and cyber breaches
2. **Limit information system access to authorized users**, processes acting on behalf of authorized users, or devices (including other information systems).
3. **Limit information system access to the types of transactions and functions that authorized users are permitted to execute.**
4. **Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.**
5. **Verify and control/limit connections** to and use of external information systems.
6. **Control any non-public information posted or processed** on publicly accessible information systems.
7. **Identify information system users, processes acting on behalf of users, or devices.**
8. **Authenticate (or verify) the identities of those users, processes, or devices,** as a prerequisite to allowing access to organizational information systems.
9. **Monitor, control, and protect organizational communications** at the external boundaries and key internal boundaries of the information systems.
10. **Implement subnetworks for publicly accessible system components** that are physically or logically separated from internal networks.
11. **Provide protection of scientific data from ransomware** and other data integrity attack mechanisms.
12. **Identify, report, and correct information and information system flaws in a timely manner.**
13. **Provide protection from malicious code** at appropriate locations within organizational information systems.
14. **Update malicious code protection mechanisms** when new releases are available.

https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

Where Cybersecurity Was

While institutions were implementing cyber controls and cyber security programs for other reasons, there were no specific federal requirements around cyber controls for funded research

Where Cybersecurity is Going

Future cyber programs will need to be designed to satisfy the cybersecurity elements of NSPM by requiring the implementation of the 14 safeguarding protocols and procedures found on Slide 20

Foreign Travel Security

NSPM-33 may require the development of new policies and procedures around travel

- As a part of their travel policy, institutions should consider
  - an organizational record of covered international travel by faculty, staff and students (e.g., travel to conferences, meetings, lectures)
  - A disclosure and authorization requirement in advance of international travel
  - Security briefings for those who are traveling
  - Assistance with electronic device security (smartphones, laptops, etc.)
    - This may include not bringing institutional devices overseas
  - Pre-event registration requirements.

https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

Research Security Training

NSPM-33 lays out guidance for what should be included in agency research security programs

- As part of their research security programs, research organizations should consider
  - Providing training to relevant personnel on research security threat awareness and identification (including insider threat training where applicable)
  - Incorporating research security into existing responsible and ethical conduct of research training
  - Conducting trainings geared toward a research security event

https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

Security Training

Federal Government Responsibilities

- Make agencies and institutions aware of the threats posed by some foreign government-sponsored efforts
- Help identify areas that have higher risk of exploitation and to reduce the burden on institutions, the government will lead on which specific trainings are required

Funding Agency Responsibilities

- Whenever possible, standardize training requirements. In instances where research agencies determine additional elements are necessary for specific research, these elements must be clearly articulated in the R&D award terms and conditions

Institution Responsibilities

- Provide the trainings
- Document the completion of the trainings
- Monitor training compliance
- Identify a designated research security point of contact (POC) and provide publicly accessible means to contact this individual

Where Training Was

No specific requirements on training listed at the federal level

Where Training is Going

Institutions will provide training on research security threat awareness and identification, including the signs to look for from an internal threat. Institutions should consider incorporating research training into existing training around research ethics. Personnel should be trained for the event of a research emergency

Export Control Training

- Agencies should require that research organizations conducting R&D that is subject to export control restrictions provide training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators and partnerships, and for ensuring compliance with federal export control requirements and restricted entities lists.

https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

What is Export Control

Export Controls are federal regulations that govern how technology, technical data, technical assistance, and items or materials (from software to satellites and more) are physically or electronically exported, shipped, transmitted, transferred, or shared from the US to foreign countries, persons, or entities.

These laws protect national security and US foreign policy interests, prevent terrorism and the proliferation of weapons of mass destruction, and preserve US economic competitiveness. Penalties for violating these laws can be severe, both for the individual researcher and the university.

https://www.bis.doc.gov/index.php/documents/regulations-docs/142-eccn-pdf/file

When is Research Subject to Export Control:

Research may be subject to export controls for a variety of reasons including, but not limited to:

- The items, materials, technology or technical data used in the research are identified on the US export control list;
- Working with (formally or informally), or providing technical assistance to, foreign nationals from countries currently sanctioned (e.g., for trade, travel, or terrorism) by the US; and
- A research agreement (e.g., contract, award, non-disclosure agreement) limits publication of results or participation in the design, conduct, or reporting of the research based on citizenship.

https://www.bis.doc.gov/index.php/documents/compliance-training/export-administration-regulations-training/1554-ear-definitions-faq/file

Polling Question: How do you think you can help your institution with NSPM-33?

1. Perform a specialized risk assessment
2. Provide Training and Awareness
3. Provide guidance on implementing updated policies and procedures
4. Perform a cyber controls assessment

What is Internal Audit's Role?

Bring awareness and education to your institution's faculty and staff on the risks:

DARPA has already released a process for denying funding applications to high-risk researchers

This could have major research implications for institutions that are unaware of potential conflicts and have not conducted appropriate due diligence

There have already been instances where funding agencies are investigating concerns regarding foreign influence

This has led to over 100 resignations and or terminations.

The guidance is still evolving, but the risk of undue foreign influence already exists

It's important to be proactive in implementing controls

What is Internal Audit's Role in Mitigating the Risk?

Specialized Risk Assessments

- Institutions should consider conducting a risk assessment to understand whether their research portfolios contain foreign research, or their researchers have foreign relationships
  - Understanding the current relationships and universe of funders may allow the institution to better understand where risks within the research portfolio are held and what controls may need to be developed
  - Further understanding the risk may allow for the institution to better align and develop policies and procedures and target trainings to maintain compliance and reduce risk

What is Internal Audit's Role in Mitigating the Risk?

Policy and Procedure Implementation

- Policies and procedures around disclosures, COI, training, and PID requirements should be developed and widely distributed. Depending on the maturity of your institutions processes and controls, the role of Internal Audit can include:
  - Advising on leading practices for creation and communication of these new policies and procedures
  - Evaluating existing policies and procedures to validate whether they sufficiently address the current landscape
  - Validating the operating effectiveness of the processes and controls documented in the policies, including confirming whether operating unites across the institution are in compliance with the policy

What is Internal Audit's Role in Mitigating the Risk?

Training and Awareness

- Mandatory training and training on new policies and procedures should be developed and offered to all applicable faculty and staff. NSPM-33 requires specific trainings to be developed and disseminated. The documentation and retention of training completion records, training attendance, and training materials should be clearly outlined in written policy and widely distributed throughout the institution. Depending on the maturity of your institution's processes and controls, the role of Internal Audit can include:
  - Assistance in the development of new and updated trainings
  - Evaluation of the current training program and the institution's processes to track employee completion of the training
  - Assurance activities to validate that employees completed the required trainings and that appropriate enforcement occurred in instances where training was not completed

What is Internal Audit's Role in Mitigating the Risk?

Cyber Control Assessments

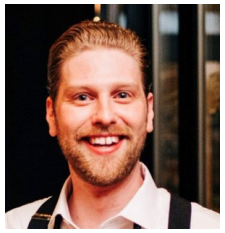
- A cyber risk and control matrix including preventive and detective controls as well as a testing plan should be developed and internal control testing around cyber controls, disclosure requirements and other applicable NSPM-33 requirements should be tested on an ongoing basis throughout the institution. The development of internal controls with preventive and detective components are essential to risk mitigation in NSPM-33 compliance. Internal Audit can work with University IT and the Chief Information Security Officer to:
  - Perform a comparison of the institution's existing cyber controls and the controls included in the Implementation Guidance for NSPM-33
  - Evaluate the operating effectiveness of the implemented cyber controls related to research and data protection

What is Internal Audit's Role in Mitigating the Risk?

Ongoing Advisory Services

- Internal audit should work closely with compliance and research teams to conduct ongoing risk assessments and internal control testing.
  - The NSPM-33 process is iterative, compliance with the stated regulations should be monitored on an ongoing basis and policies and procedures should be updated based on new guidance, new operations, and lessons learned as the institution implements their NSPM-33 program.

Questions?



Dillon Clark
dilclark@deloitte.com

Elizabeth Walton
elwalton@deloitte.com

Announcements

Upcoming ACUA Webinar

Month	Date & Time	Presenter	Topic
February	2/22/24 1:00pm EST	Diligent	Fraud Affecting Universities in a Post-Covid/Hybrid World

ACUA VIRTUAL
SPRING SUMMIT
Auditor To Trusted Advisor

Registration now open!

New Kick Starter Available!

Banner User Access

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 February 15th!

Presidents Expense Review

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

Will be available in the members-only Audit Tools

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.

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.

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.

Get Educated

- Take advantage of the several FREE webinars held throughout the year.
- Attend one of ACUA conferences:
  ACUA Spring Virtual Summit
  AuditCon (September 2024)
- Contact ACUA Faculty for training needs.

ACUA WEBINARS

Join us for our upcoming webinar.

Thank You