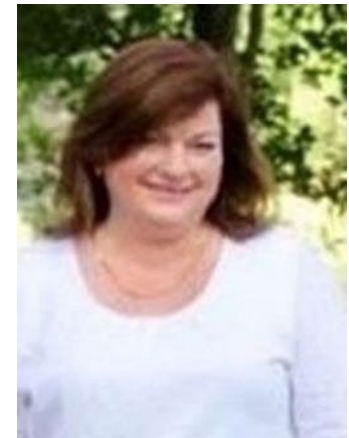


- Don't forget to connect with us on social media!



ACUA Virtual Learning Director
Lisa Gendusa
Internal Auditor
Texas State University System



ACUA Virtual Learning Volunteer
Connie Applebach
Auditor III
University of Houston System



CPE credit

This webinar qualifies for 1 hour of CPE credit

To qualify for the credit:

- You must be in attendance for the entire webinar
- You must participate in the polling questions
- Complete the evaluation form at the end of the webinar

Qualified attendees will receive their CPE certificate via email in 3-4 weeks

Questions regarding the CPE for this webinar can be sent to:

- info@acua.org

Research security: what auditors must know in 2022

ACUA
June 2, 2022



INTRODUCTION

Meet the presenters



Matt Gilbert

CISA, CRISC, CMMC PA
Cyber/IT & CMMC Leader
Principal
Baker Tilly



Mike Cullen

CISA, CISSP, CIPP/US, CMMC PA
Cyber/IT Higher Ed Leader
Principal
Baker Tilly



Adrienne Larmett

CRA, MBA
Risk Advisory Higher Ed Leader
Principal
Baker Tilly

Connect with Baker Tilly

Higher education insights

www.bakertilly.com/industries/higher-education

Cybersecurity insights

www.bakertilly.com/specialties/cybersecurity



Agenda

Research security challenges

Regulatory and compliance requirements

Challenging requirements for academia

Addressing challenges and requirements

Discussion on specific impacts to participants





Overview

- Complex terms related to research security are cropping up across the spectrum of research agreements
- It is difficult to figure out what requirements apply to each agreement as there are so many disparate security terms
- It is important to work across the research community to create effective understanding, systems and controls to protect research data

A cityscape at dusk with a prominent skyscraper on the left and a body of water on the right. The sky is a mix of purple, pink, and blue. The buildings are lit up, and the water is dark with some reflections.

Learning objectives

At the end of the workshop, participants will:

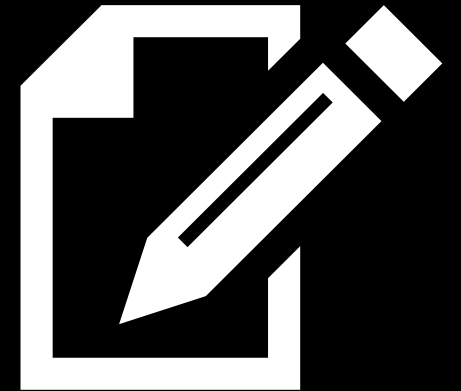
- Understand the latest research security developments and how it impacts higher education
- Gain insight into your specific questions on these developments and specific requirements that impacts your institution
- Take away a list of challenging requirements and potential solutions

Polling question

Question #1

Does your institution conduct a large amount of funded research?

- a. Yes
- b. No
- c. I don't know

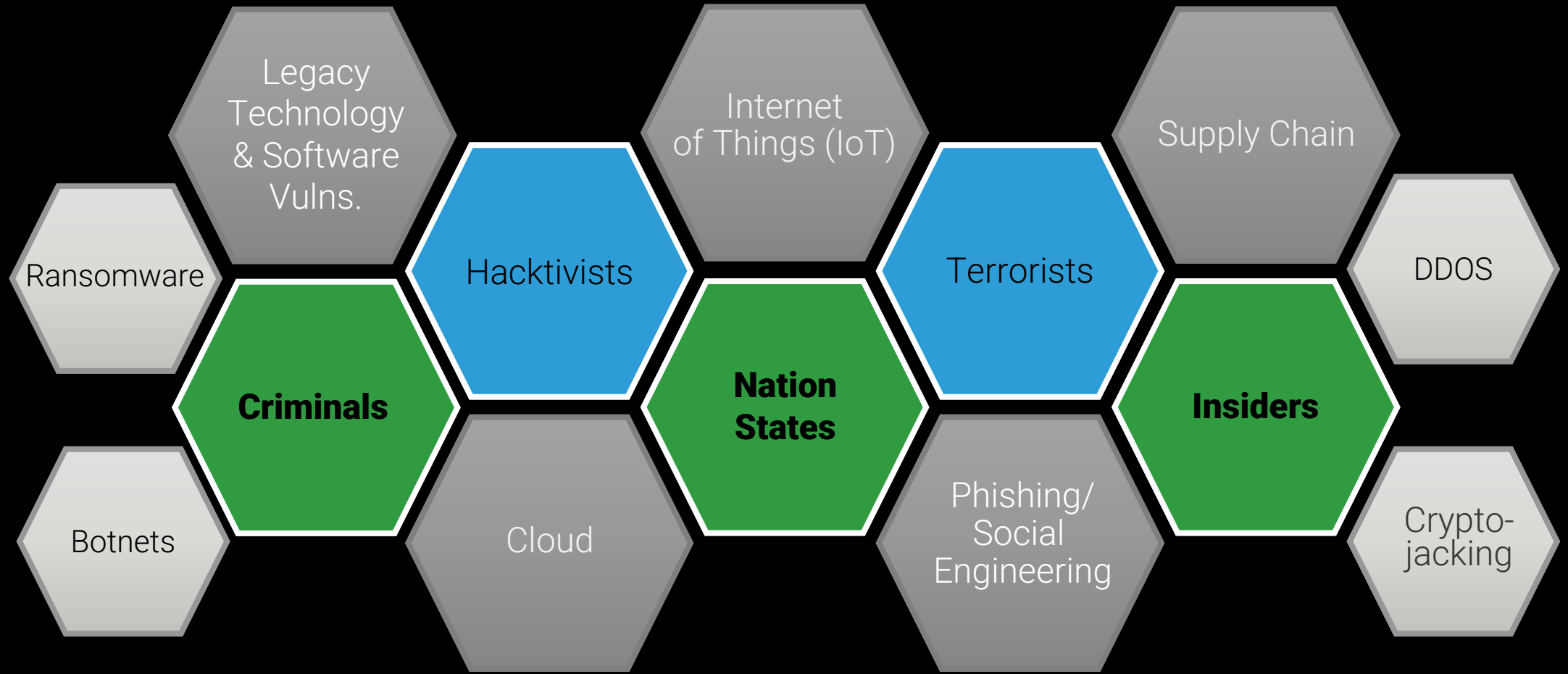


A short, solid yellow horizontal bar.

Research security challenges



Threats



Risks

Reputation

Damage to brand/negative publicity

Damage to individual faculty/researcher professional standing

Competitive

Loss of intellectual property

Damage to relationships with partners (e.g., research sponsors, other institutions)

Operational

Loss of time spent to respond

Loss of ability to operate or continue work

Financial

Cost of response for incidents

Loss of future funding/debarment

Regulatory

Cost to address requirements

Cost of fines, sanctions

Legacy perceptions

Researchers/PIs

- My funding, my way
- Data will be published, no need for security
- Regulations are guidelines, not requirements
- Do it “cheaper” buying/building own systems
- Mandatory training is useless

Support professionals

- Institution must be 100% compliant
- Research data should be treated the same as sensitive/confidential enterprise data
- Researchers should follow policies/procedures
- Only certain research covered by IRB or export controls really needs protections

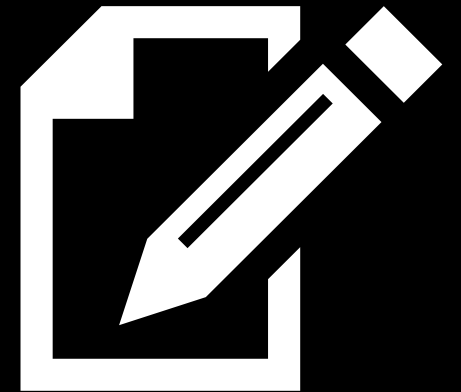


Polling question

Question #2

What do you view as the greatest risk related to research at your institution?

- a. Reputation
- b. Competitive
- c. Operational
- d. Financial
- e. Regulatory



Regulatory and compliance requirements



Example items where research data security requirements show up

Contracts and subcontracts

Grants and sub-awards

Cooperative agreements

Data use agreements (DUA)

Data management plans (DMP)

Data licenses

Human subject protocols

Technology control plan (TCP)

Confidential and non-disclosure agreements (CDA/NDA)

Material transfer agreements (MTA)

Memoranda of understanding (MOU) with external parties

Business associate agreements (BAA)

Examples of regulatory requirements

Federal Acquisition Regulation (FAR) 52.204-21: basic safeguarding

Department of Defense FAR Supplement (DFARS) clauses: 252.204-7012, 7019, 7020

Department of Defense Cybersecurity Maturity Model Certification (CMMC)

National Security Presidential Memo (NSPM) 33

Department of Justice Cyber Civil Initiative

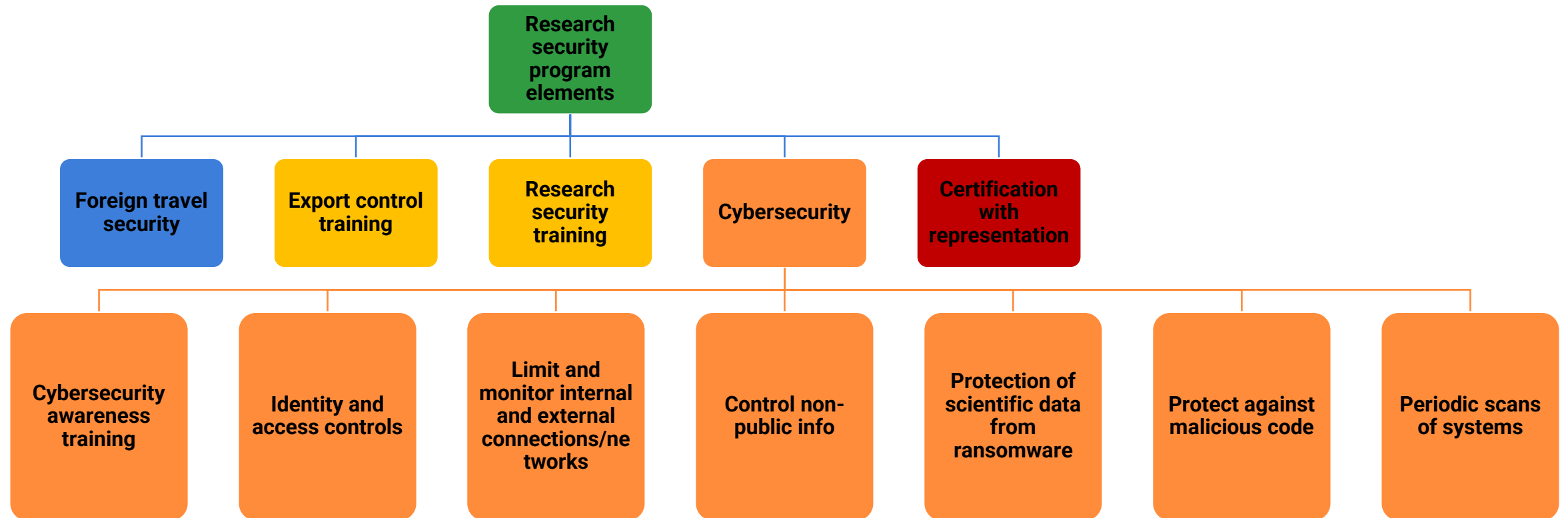
Export controls (EAR/ITAR/FACR)

NIH data management and sharing policy

Health Insurance Portability and Accountability Act (HIPAA)


European Union General Data Protection Regulation (GDPR)

NSPM-33



Export controls compliance program elements



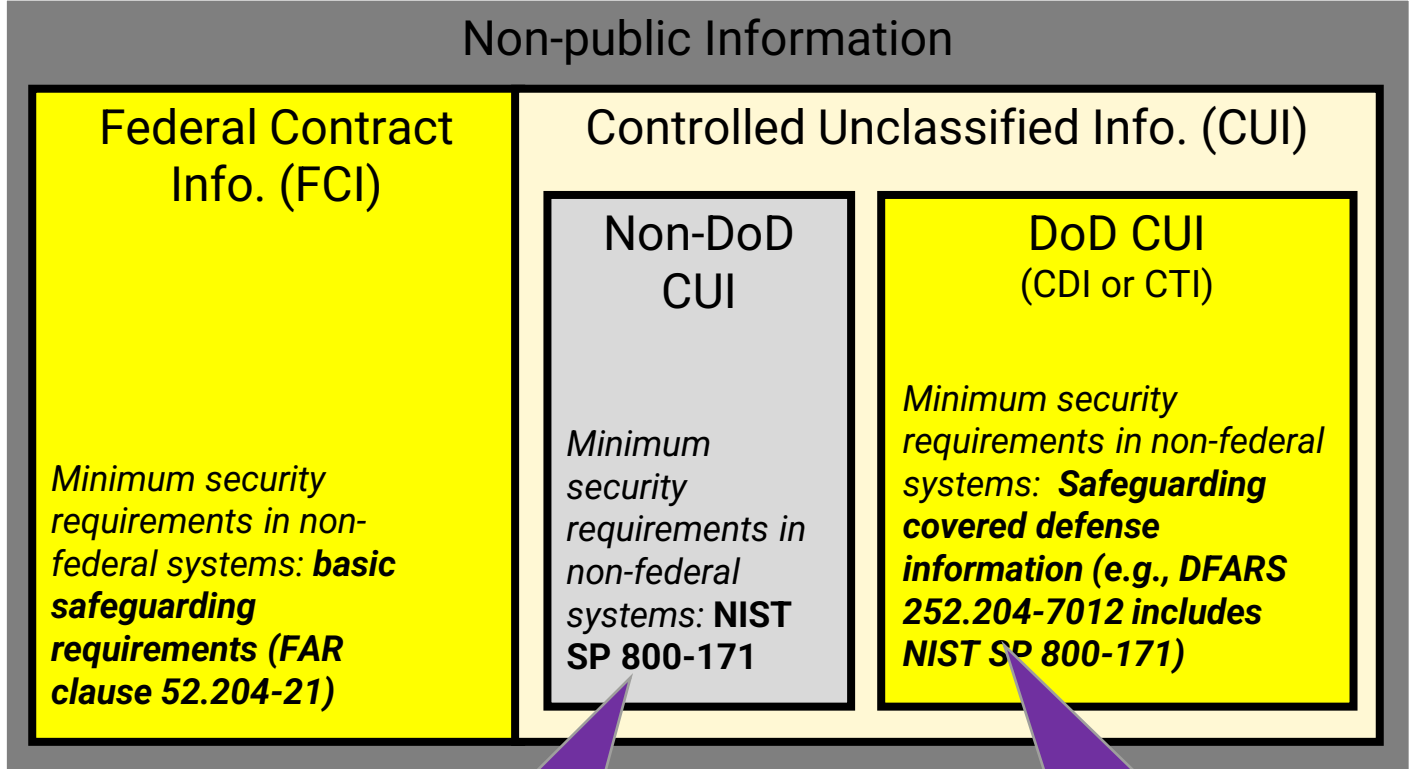
 *Elements that map/align to other regulatory cybersecurity requirements*

FAR/DFARS: Recap on federal data

CMMC applies to FCI & CUI in DoD work

Public Information

No minimum security requirements, as this is information to be shared with the public.



Classified Information

*The National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that the cleared U.S. defense industry protects the **classified information** in their possession while performing work on contracts, programs, bids, or research and development efforts.*

FAR Case 2017-016 for CUI still in progress

DFARS Interim Rules 7019, 7020 Effective 12/1/20

CMMC: DoD and CMMC AB updates

DoD

CMMC
AB

Version 2.0
released with
new assessment
and scoping
guides

Lack of FY21
pilot
procurements

Program moved
from
undersecretary
for acquisition
and sustainment
to DoD CIO

New permanent
staffing

New training for
V2.0

Department of Justice civil cyber-fraud initiative

Use the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients



Hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols or knowingly violating obligations to monitor and report cybersecurity incidents and breaches



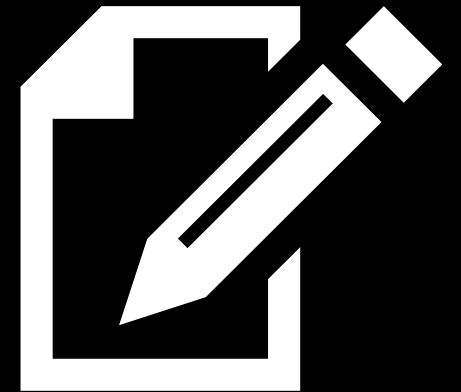
Work closely with other federal agencies, subject matter experts and its law enforcement partners throughout the government.

Polling question

Question #3

Has your institution started the process of becoming CMMC compliant?

- a. Yes
- b. No
- c. I don't know





Challenging requirements for academia



Challenge: governance and enclaves

Governance

- Who will “own” the research security?
- Who are the stakeholders?
- Who funds the program?

Research silos

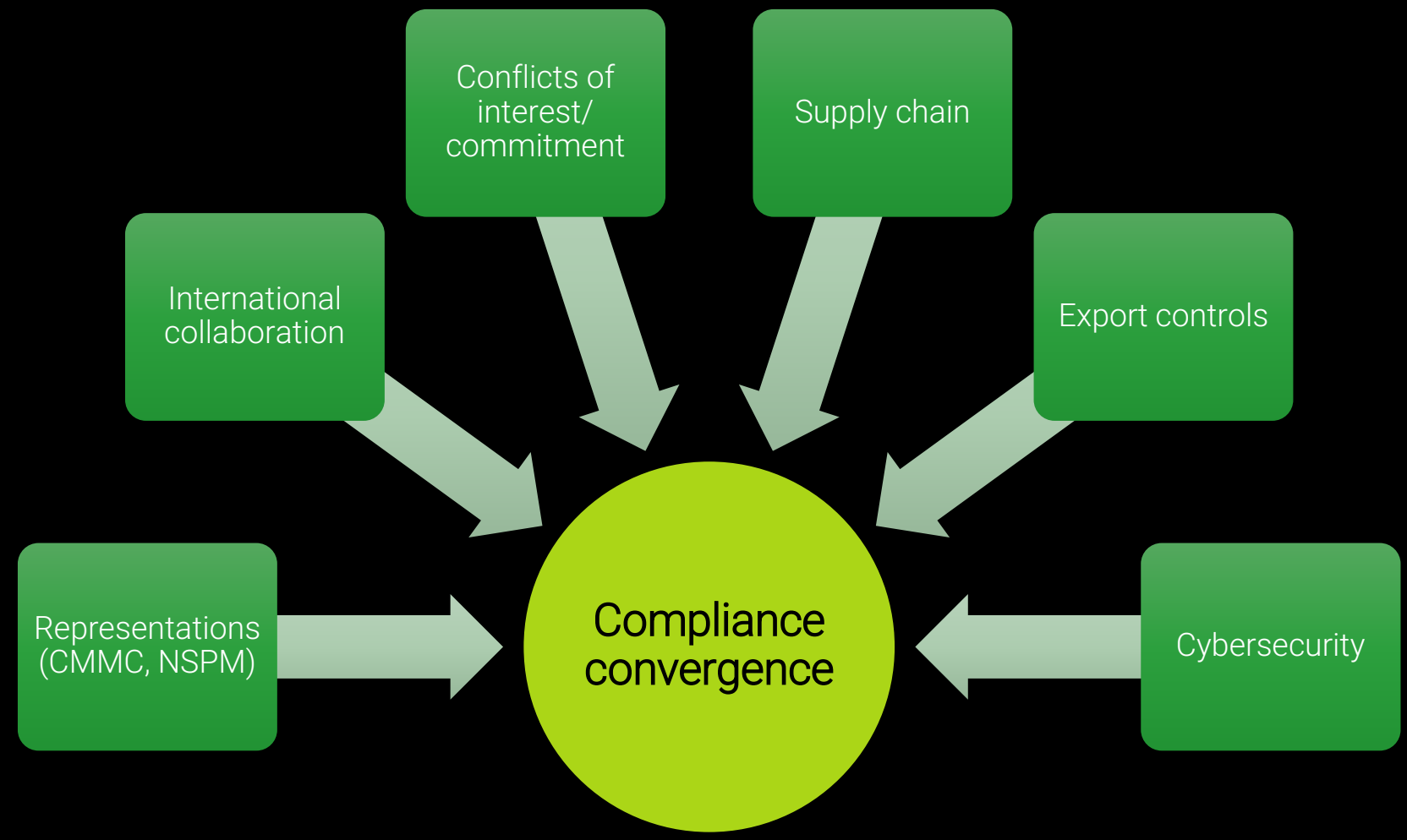
- Who manages compliance?
- Who are the typical sponsors?

Technology

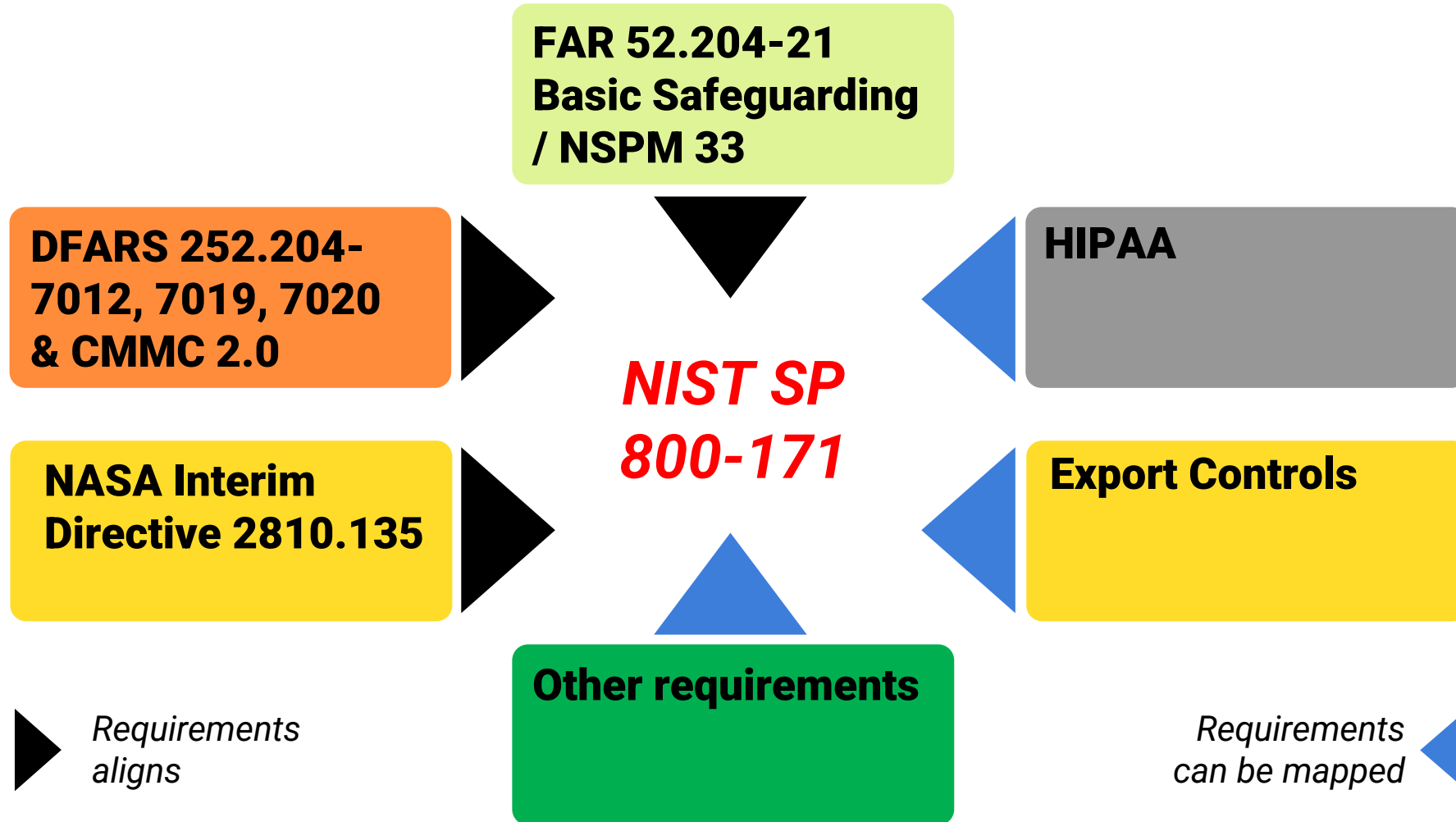
- Who buys/builds solution?
- Cloud? On-premises? Special equipment?



Challenges: future requirement trends



Potential framework



Addressing challenges and requirements



People response: governance stakeholders

Research Focus

Faculty/Researchers/PIs

Research Leadership (Provost, VP/VC)

Deans/Dept. Heads

Institutional Review Board

Library

Tech Transfer/Commercialization

Research Admin/Compliance/Integrity

Support Focus

Information Technology

Information Security

General Counsel

Procurement

Privacy

Risk Management

Env. Health Safety

Process response: key elements

Culture and values (tone at the top)

Risk assessment and management

Policies and standards

Outreach and education

Monitoring and evaluation

Audits and investigations

Improvements and changes



Technology response: key elements

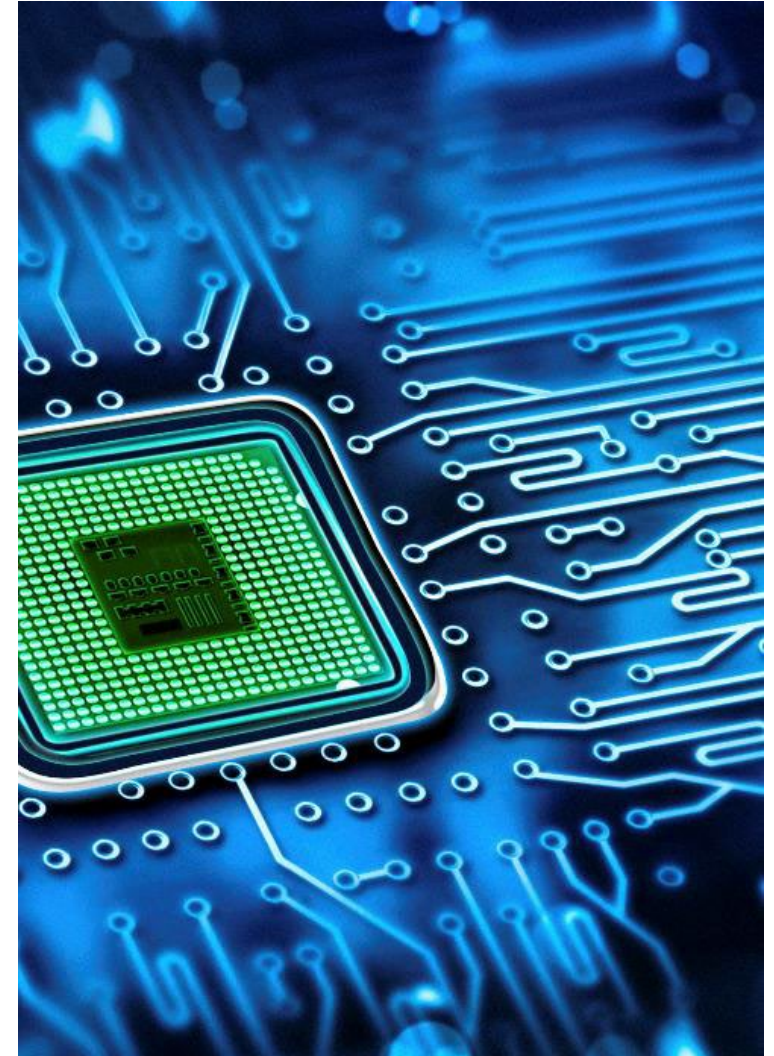
Multi-factor authentication

Anti-malware/virus/ ransomware

Network segmentation

Security event monitoring

Collaboration tool controls



Discussion on specific impacts to participants

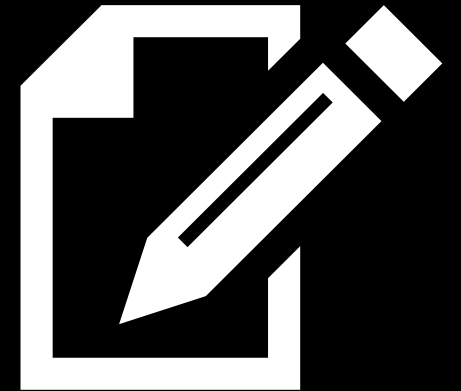


Polling question

Question #4

Has your institution's internal audit performed any reviews related to research data security?

- a. Yes
- b. No
- c. I don't know



THANK YOU!

Connect with us



Matt Gilbert

matt.gilbert@bakertilly.com



Mike Cullen

mike.cullen@bakertilly.com



Adrienne Larmett

adrienne.larmett@bakertilly.com

The background features a network of glowing blue and white icons (person, envelope, speech bubble, location pin) connected by lines, overlaid on a blurred image of a globe. A central black rectangle contains white text.

Connect with us

Subscribe to receive higher education alerts and event invitations:

connect.bakertilly.com/subscribe

Subscribe to our **Higher Ed Advisor** podcasts:

connect.bakertilly.com/higher-ed-advisor-podcast



Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly US, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

© 2022 Baker Tilly US, LLP



Future CPE events coming your way!

Webinars

June 23, 2022 – Ft. Hill – Construction auditing

July 28, 2022 – ACUA's Sideline Committee – Auditing Athletics

August 11, 2022 – Data Analytics

August 25, 2022 – Auditing Retroactive Withdrawals or Hardship Petitions

AuditCon

September 11 – 15, 2022

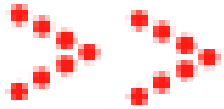
Las Vegas, NV



Did you know that Connect ACUA allows you to post new messages directly from your email without logging in to the Connect ACUA website?

For more details, check out the Quick Tip post on [Connect.ACUA.org](https://connect.acua.org)

Your Higher Education Auditing Connection

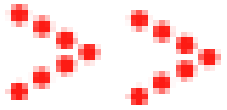


Latest Kick Starter Released!

Budget Process

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



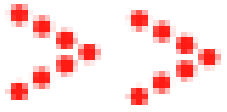


Next Kick Starter Release is June 15th!

NCAA Compliance – Head Coach Responsibilities

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





ACUA Kick Starters

Use a Kick Starter to launch your next audit!

- Developed by ACUA members with subject matter expertise
- Focused on higher education specific topics

<https://acua.org/Audit-Tools/ACUA-Kick-Starters>



Do you have a great idea for an ACUA Kick Starter? Contact Lily Ly at lilyly@aa.ufl.edu.



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 our upcoming conferences:
Audit Interactive
Denver, CO
March 27 – 27, 2023

AuditCon
September 11 – 15, 2022
Las Vegas, NV
- 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 us



www.ACUA.org

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.