ACUA WEBINARS

Third-Party Risks and Relationships Management

June 22, 2023

ACUA WEBINARS

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

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

ACUA SOCIAL NETWORKING

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

ACUA Virtual Learning Volunteer
Jonathan Stadig
Senior Auditor
University of Massachusetts

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

Third-Party Risks and Relationships Management

Rob Clark, Jr., CIA, CCEP, CBM

Chief Audit & Compliance Officer

Howard University

Robert.Clark@howard.edu

https://www.linkedin.com/in/robclarkjr/

www.RobClarkJr.com

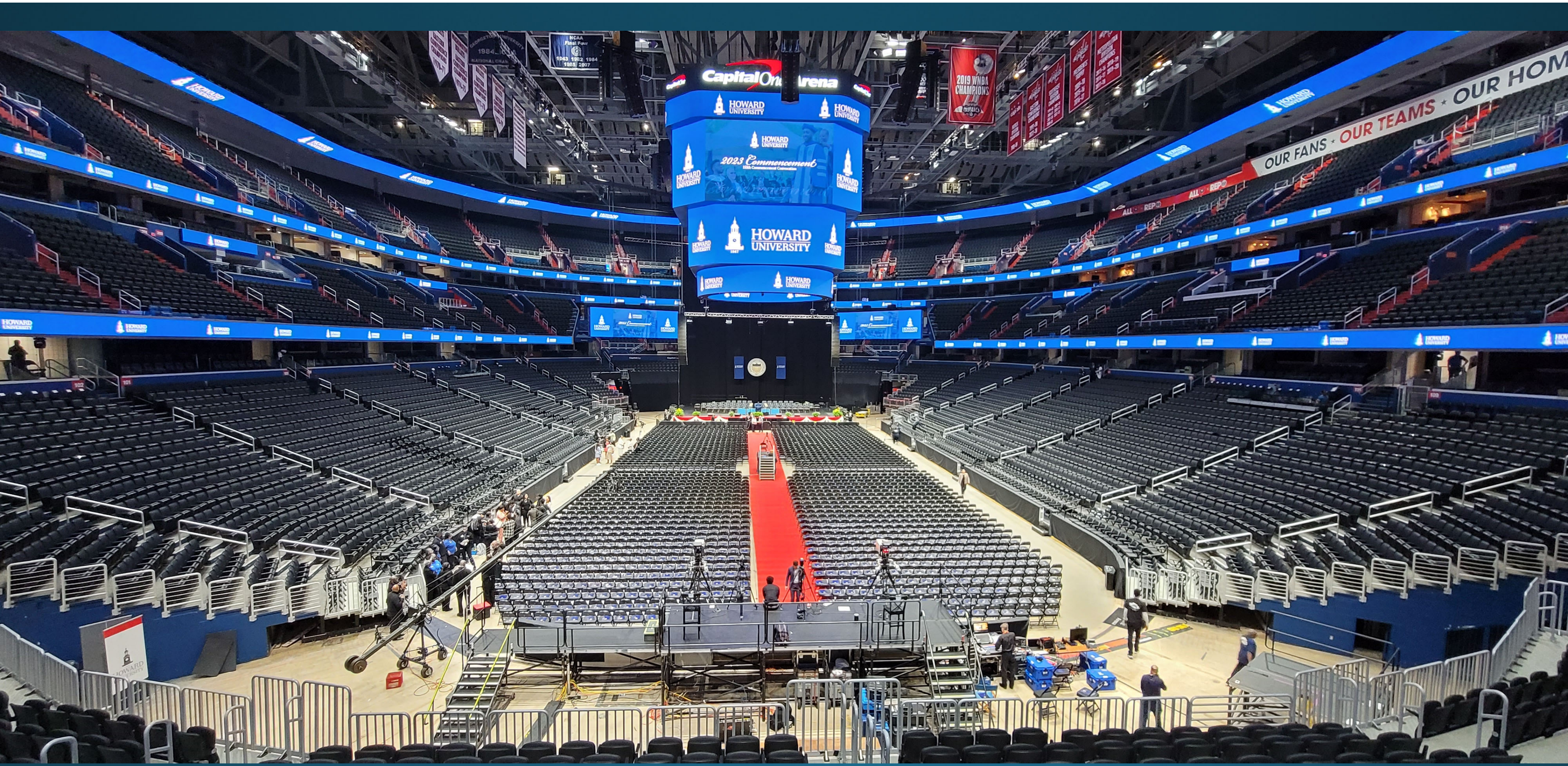
770.815.7922

What’s your “Why?”

156

2,000

Capital One Arena
HOWARD UNIVERSITY
The Honorable Joseph R. Biden, Jr. The 46th President of the United States of America
OUR FANS · OUR TEAMS · OUR HOME
1984 NCAA NATIONAL CHAMPIONS
NCAA Final Four 1943 1982 1984 1985 2007
2019 WNBA CHAMPIONS


Capital One Arena
HOWARD UNIVERSITY
2023 Commencement
HOWARD UNIVERSITY
2019 WNBA CHAMPIONS
OUR FANS ★ OUR TEAMS ★ OUR HOM
NCAA Final Four

Capital One Arena
HOWARD UNIVERSITY
The Honorable Joseph R. Biden, Jr. The 46th President of the United States of America
OUR FANS · OUR TEAMS · OUR HOME
2019 WNBA CHAMPIONS
1984 NCAA NATIONAL CHAMP

Objectives of the Session

- Understand concepts of third-party risks and relationships management
- Review of risks and risk mitigation over third-parties
- Discussion of effective practices for managing third-party risks and developing

Who cares?

- Why does this matter?
- Isn’t this just all “legal stuff”?
- Why don’t we just leave this to the lawyers to work out?

Polling Question 1:
What is your role in managing third-party management?

A. No clue… I leave that up to the Purchasing and Legal folks

B. I have some responsibility to monitor that contracts are appropriately established and followed

C. I am involved in the whole shebang – from negotiating the contract to monitoring for compliance

D. I audit and assess the people who manage third-parties

ERM COSO Framework - "Enterprise Risk Management -- Integrating with Strategy and Performance"

Define the organizational structure, board policies, management risk appetite

Define objectives for strategy, operations, reporting, & compliance

What **could** go wrong?

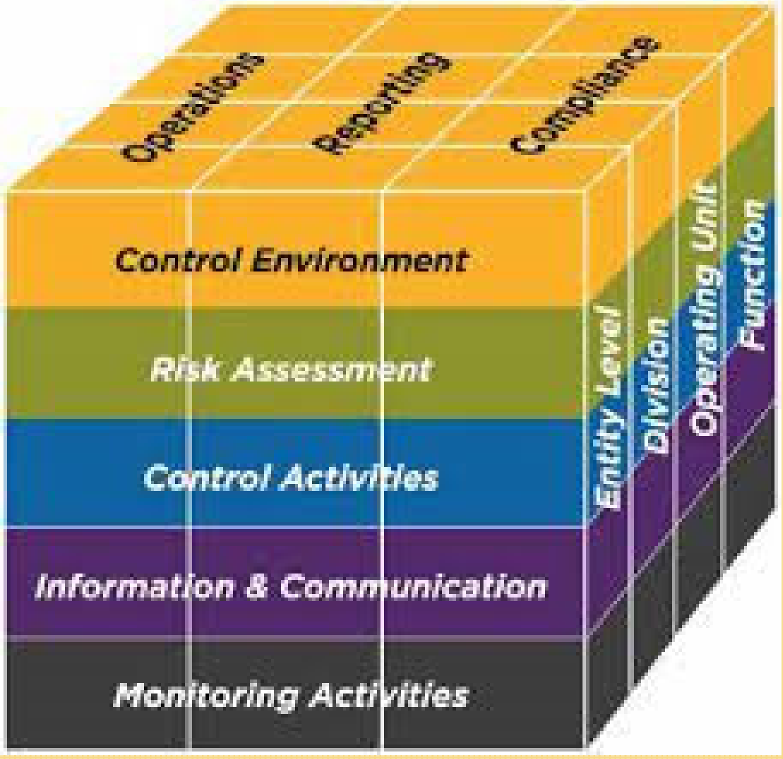
What is the **impact** and **likelihood** of risks?

How to manage risk: Share it, avoid it, reduce it, or accept it

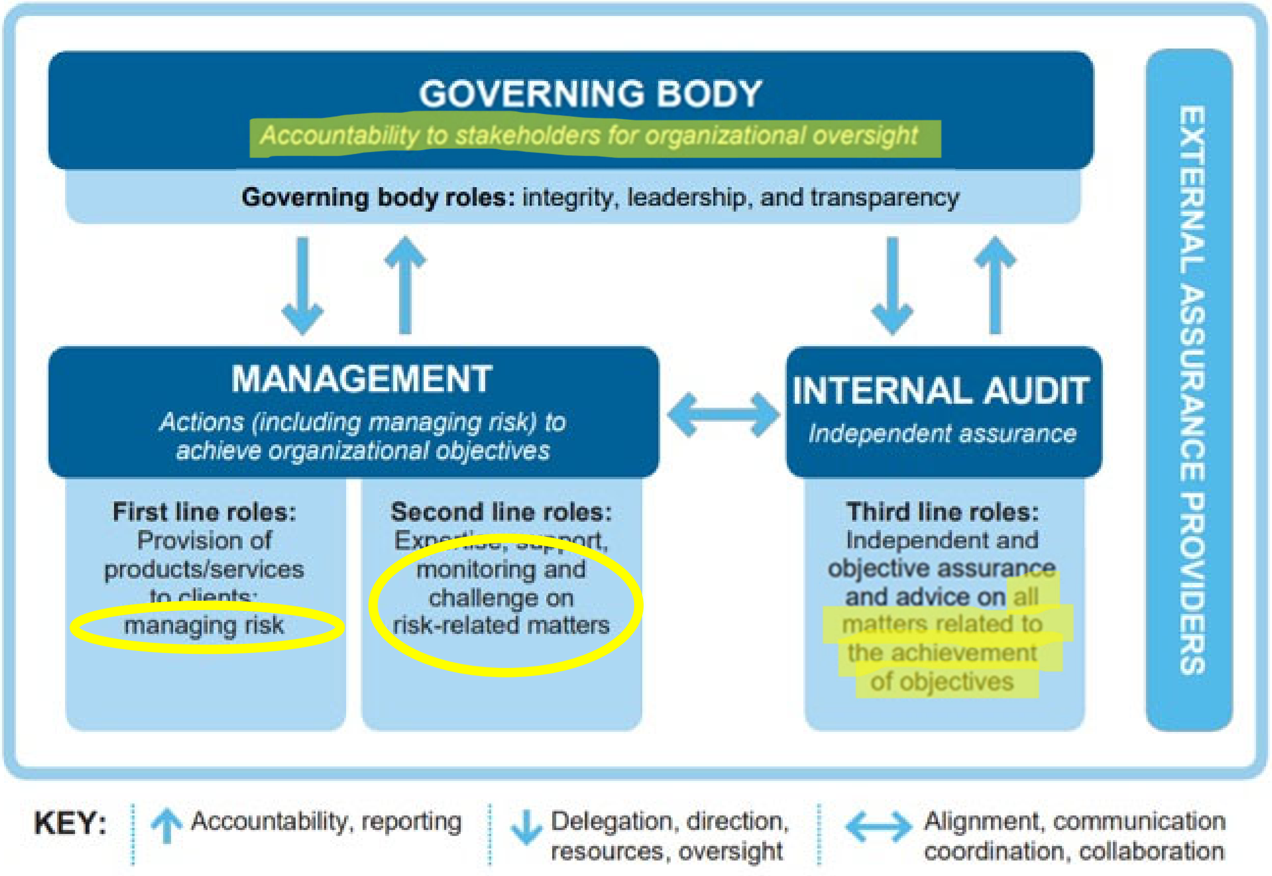
Procedures to ensure effective risk mitigation

Education & awareness of effective policies and practices

Management reviews & audit assesses



The IIA's Three Lines Model



GOVERNING BODY

Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT

Actions (including managing risk) to achieve organizational objectives

First line roles: Provision of products/services to clients; managing risk

Second line roles: Expertise, support, monitoring and challenge on risk-related matters

INTERNAL AUDIT

Independent assurance

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

KEY: ↑ Accountability, reporting | ↓ Delegation, direction, resources, oversight | ↔ Alignment, communication coordination, collaboration

Source: Institute of Internal Auditors

Risk Assessment Discussion Tool

Category of Risk	Risk Description (Explanation of Threat)	Potential Impact [1 (low) to 5 (high)]	Likelihood [1 (low) to 5 (high)]	Risk Rating	Primary Point of Contact to Mitigate Risk	Current Strategies for mitigating the risk	What Monitoring is in place
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			
				0			

Types of Third-Parties

- **Services** (e.g., technology services, contractors, consultants, service providers, dining, housing, transportation, public safety, etc.)
- **Products** (e.g., office supplies, furniture, printing services)
- **Sponsored Programs**
- **Financial services providers**
- **Fundraising services, etc., etc.**

Polling Question 2:
How many third-party vendors do you have at your institution?

A. 1 – 100

B. 101 – 500

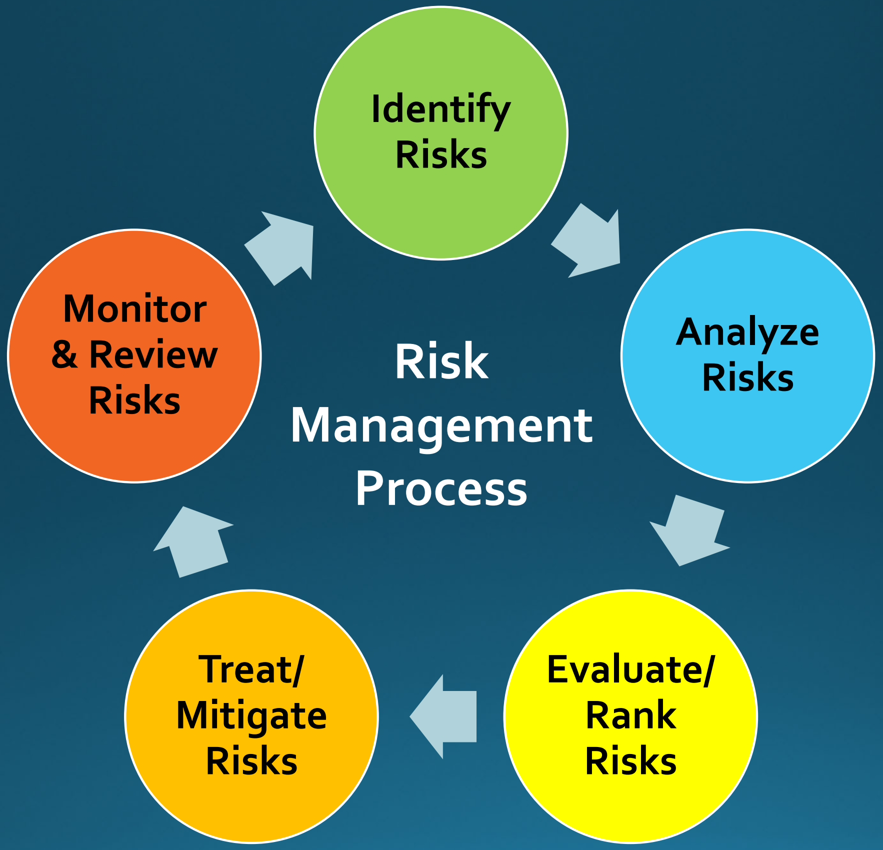
C. 501 – 1,000

D. 1,000 +

What are the numbers?

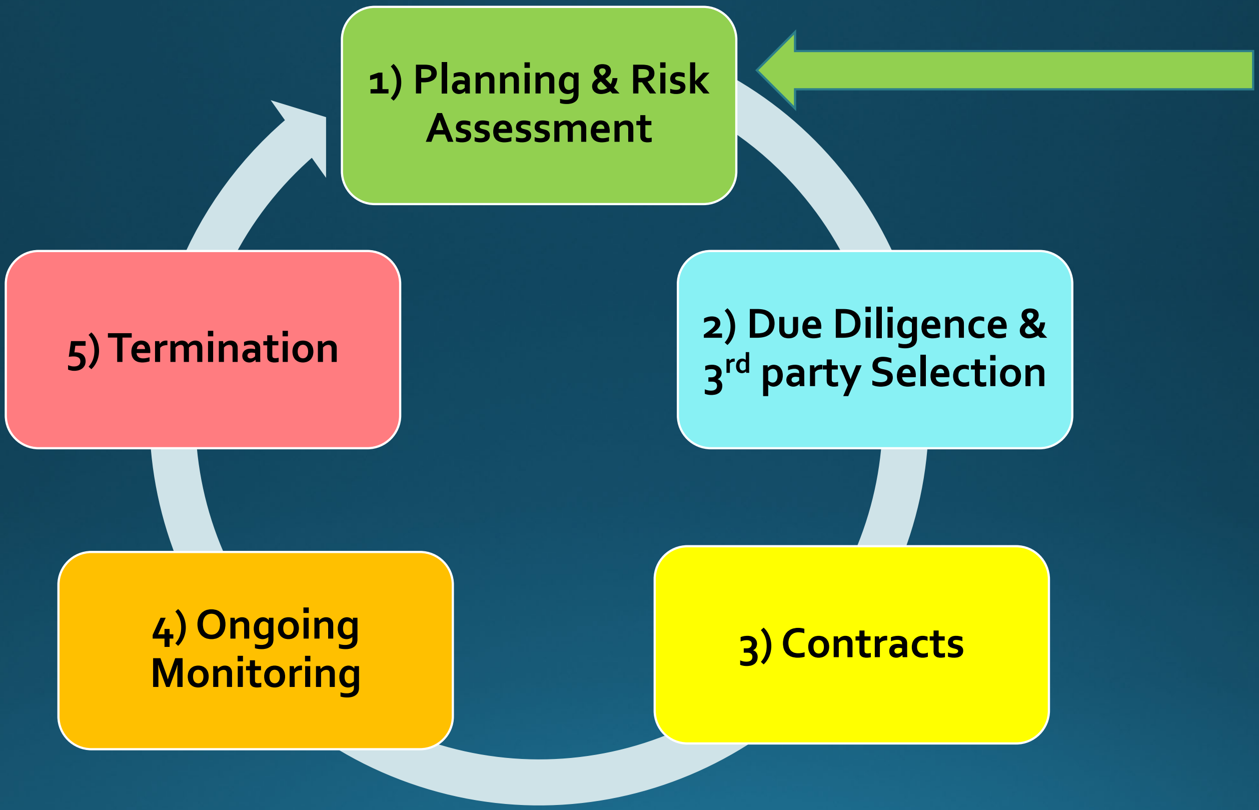
- Not uncommon for a large university to have between 20,000 to 40,000 contracts with third-parties
- Estimated 60-80% of university transactions are governed by contracts with third-parties
- Many of these contracts contain clauses, terms, conditions, commitments and milestones
- Who is managing and tracking these?

Risk Management Process



Robert Clark, Jr., CCEP, CIA, CBM, Chief Audit & Compliance Officer, Howard University © 2023

5 Phases of Third-Party Monitoring


1) Planning & Risk Assessment

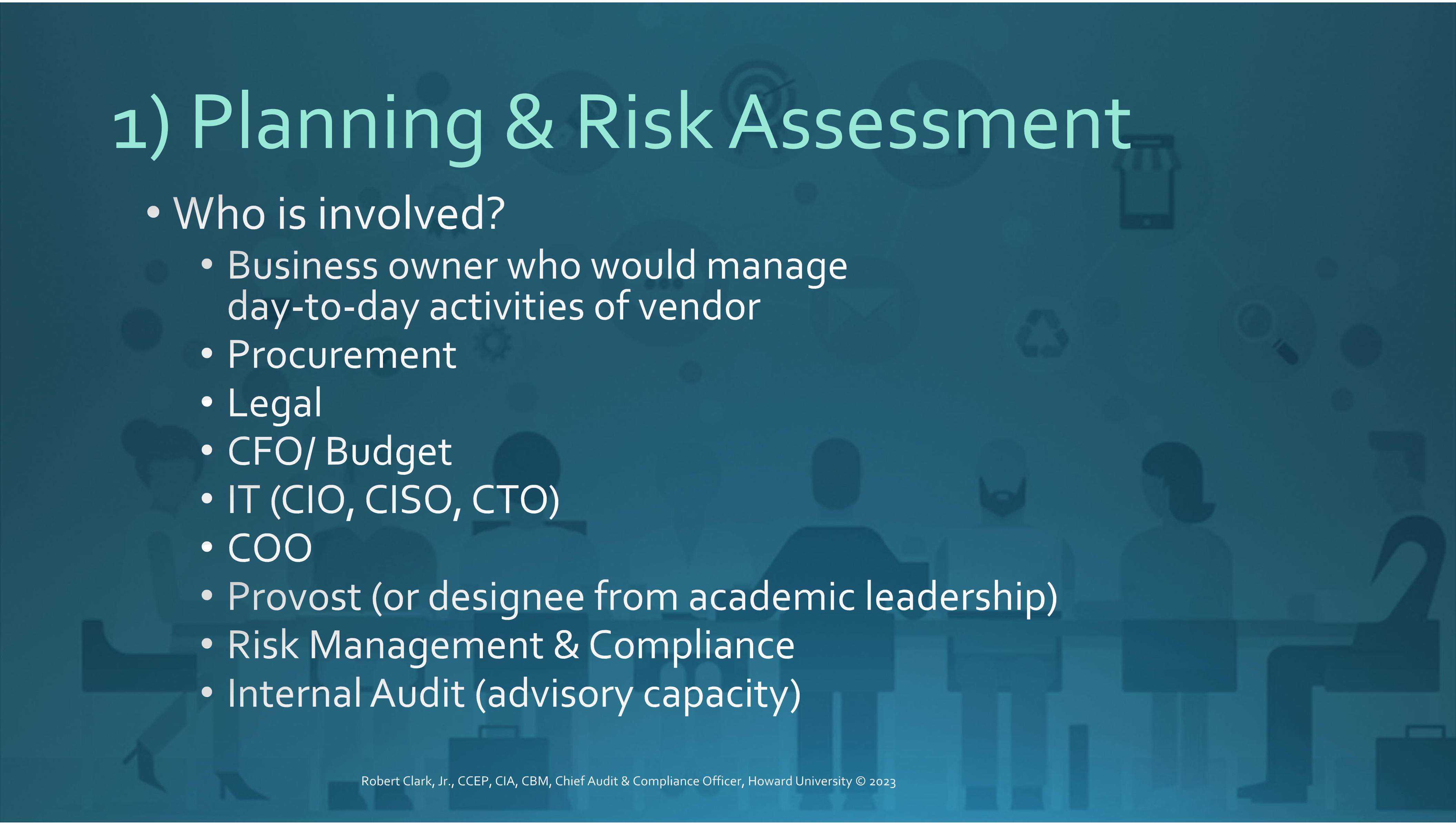
2) Due Diligence & 3rd party Selection

3) Contracts

4) Ongoing Monitoring

5) Termination

Robert Clark, Jr., CCEP, CIA, CBM, Chief Audit & Compliance Officer, Howard University © 2023



1) Planning & Risk Assessment

- Who is involved?
  - Business owner who would manage day-to-day activities of vendor
  - Procurement
  - Legal
  - CFO/ Budget
  - IT (CIO, CISO, CTO)
  - COO
  - Provost (or designee from academic leadership)
  - Risk Management & Compliance
  - Internal Audit (advisory capacity)

1) Planning & Risk Assessment

- How does the vendor line up with your core values?
- How would this vendor align with your strategic goals?
- How critical are the services being proposed by the third party (Tier 1, 2, 3)?
- Will the third-party have access to your sensitive information?
- Will the third-party have access to your offices or direct interaction with your customers?
- Will they be using any subcontractors of their own to provide services to you (i.e., your ‘fourth parties’)?

IT Governance Council

The purpose of an IT Governance Council is to provide oversight, strategic direction, and decision-making authority for IT-related matters within the organization. The council consists of senior leaders, executives, and representatives from various business units and functions within the organization.

Focus of IT Governance Council

1) **Strategic alignment**: The council ensures that the organization's IT strategy aligns with its overall business strategy and objectives. It helps prioritize IT initiatives and investments to support the organization's goals and maximize value.
2) **Risk management**: The council identifies and assesses IT-related risks and establishes risk management strategies and controls to mitigate those risks. It ensures that appropriate security measures, compliance standards, and disaster recovery plans are in place.
3) **Resource allocation**: The council advises on the allocation of IT resources, including budget, personnel, and technology infrastructure. It evaluates proposals for IT projects and initiatives, making recommendations to senior leadership on priorities, funding, and resource allocation.

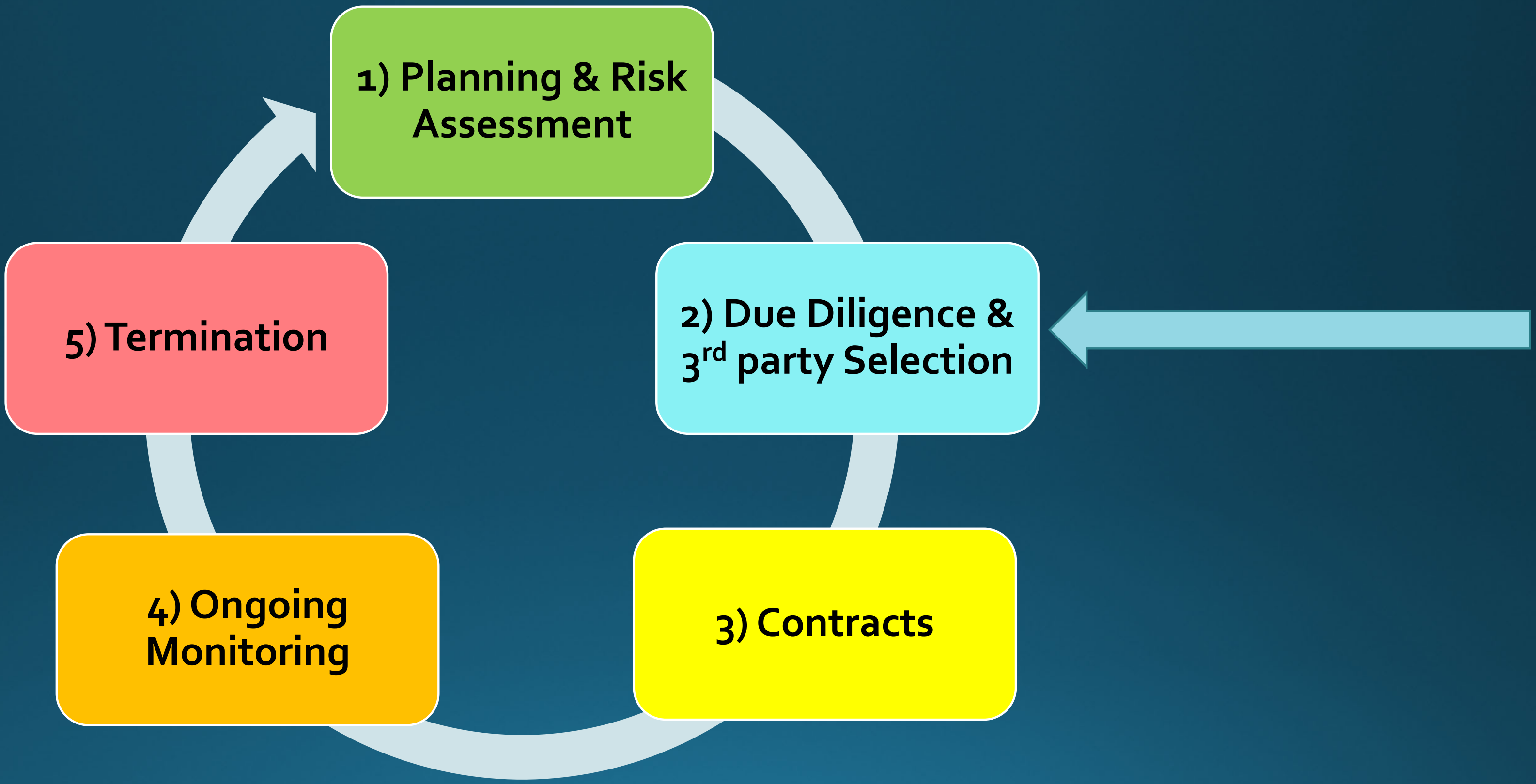
Focus of IT Governance Council

4) **IT policy development**: The council establishes and reviews IT policies, standards, and guidelines to ensure compliance, consistency, and best practices across the organization. It helps develop IT governance frameworks, frameworks for data management, and cybersecurity protocols.

5) **Performance measurement**: The council defines key performance indicators (KPIs) and metrics to evaluate the effectiveness of IT initiatives and monitor the organization's IT performance. It reviews progress, identifies areas for improvement, and ensures accountability.

6) **Communication and collaboration**: The council facilitates communication and collaboration between IT and business units. It serves as a platform for sharing information, discussing IT-related challenges and opportunities, and fostering a culture of collaboration and innovation.

5 Phases of Third-Party Monitoring



1) Planning & Risk Assessment

2) Due Diligence & 3rd party Selection

3) Contracts

4) Ongoing Monitoring

5) Termination

2) Due Diligence

- Dun & Bradstreet (Business credit score)
- Secretary of the State
- Review SSAE 18 reports
- Review SOC 2 Type 2 reports
- Evaluate financial strength
- Check references
- Who reviews these?
- Who is involved in making decision?

SOC Reports

	WHAT IT REPORTS ON	WHO USES IT
SOC 1	Internal controls over financial reporting	User auditor and user's controller's office
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Shared under NDA by management, regulators and others
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Publicly available to anyone

SOC 1 vs SOC 2

Transaction and Security Processing Controls Focus

[Essential for Revenue Software]

TYPE 1	TYPE 2
• Organization system & controls • At a specific point in time • Key security issues • Opinion on design of controls	• Organization system & controls • Over a period of time • Opinion on design of operating effectiveness of controls

Security Controls Focus

[Essential for all service organizations Including CLOUD service providers]

TYPE 1	TYPE 2
• Organization system & controls • At a specific point in time • Focus on security	• Organization system & controls • Over a period of time • Opinion on design of operating effectiveness of controls

Check CSPs with STAR Registry

- Cloud Service Providers (CSPs) complete the CSA CAIQ (Cloud Security Alliance – Consensus Assessments Initiative Questionnaire) and CCM v4 (Cloud Controls Matrix) to submit to the STAR Registry (Security, Trust, Assurance, and Risk) Registry

While You're Asking Questions About Your Vendors…

- Demonstrate YOUR infosec program
- Build a sharable document demonstrating your program's compliance with framework
- Share **first** when asked to complete a questionnaire
- Compile external proof (SSAE 18, Shared Assessments, etc.)

Polling Question 3:
Who is involved in the due diligence for third parties at your institution?

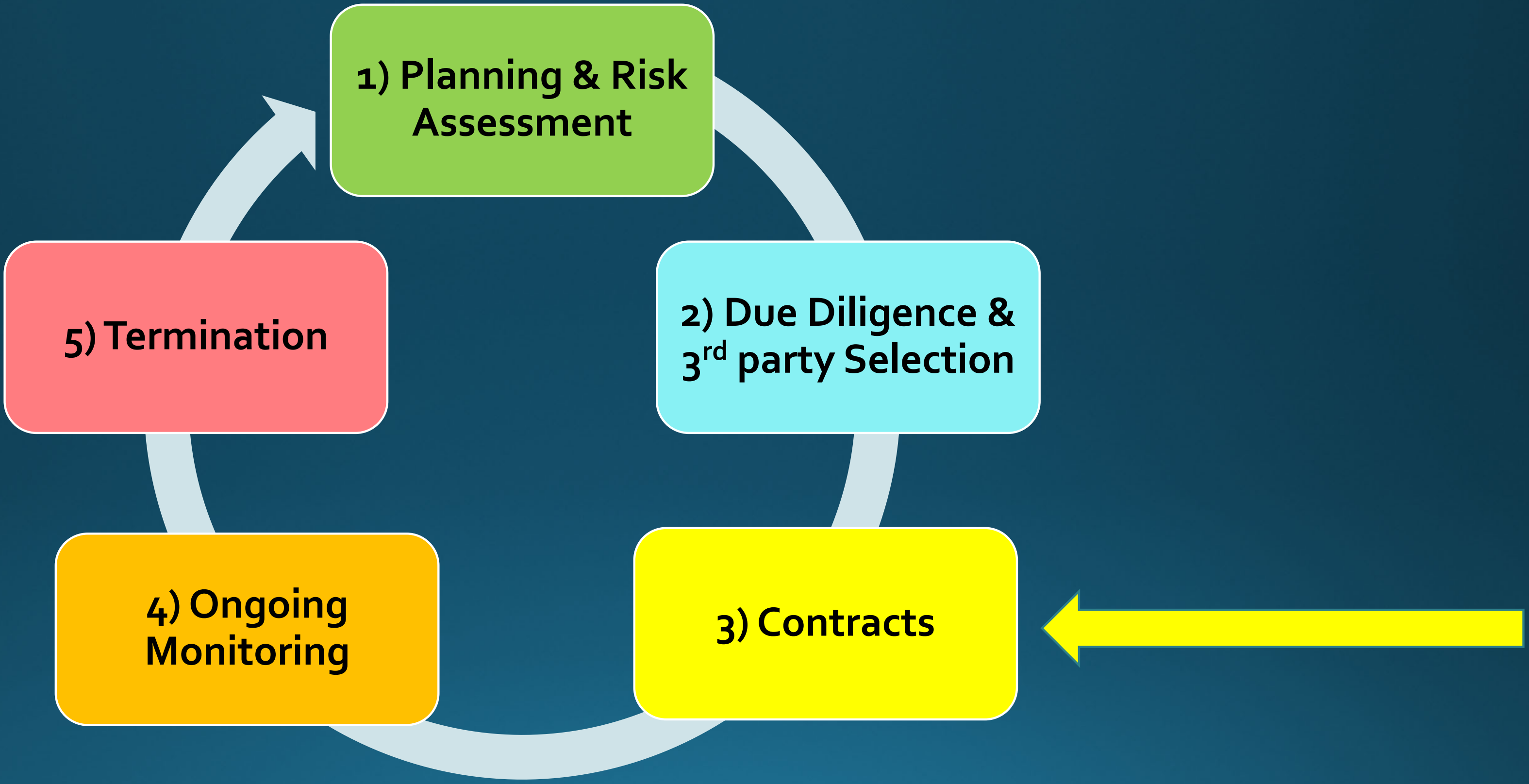
A. Purchasing

B. Purchasing and Legal

C. Purchasing, Legal, IT, (and others)

D. No clue (but I'm about to find out tomorrow!)

5 Phases of Third-Party Monitoring



1) Planning & Risk Assessment

2) Due Diligence & 3rd party Selection

3) Contracts

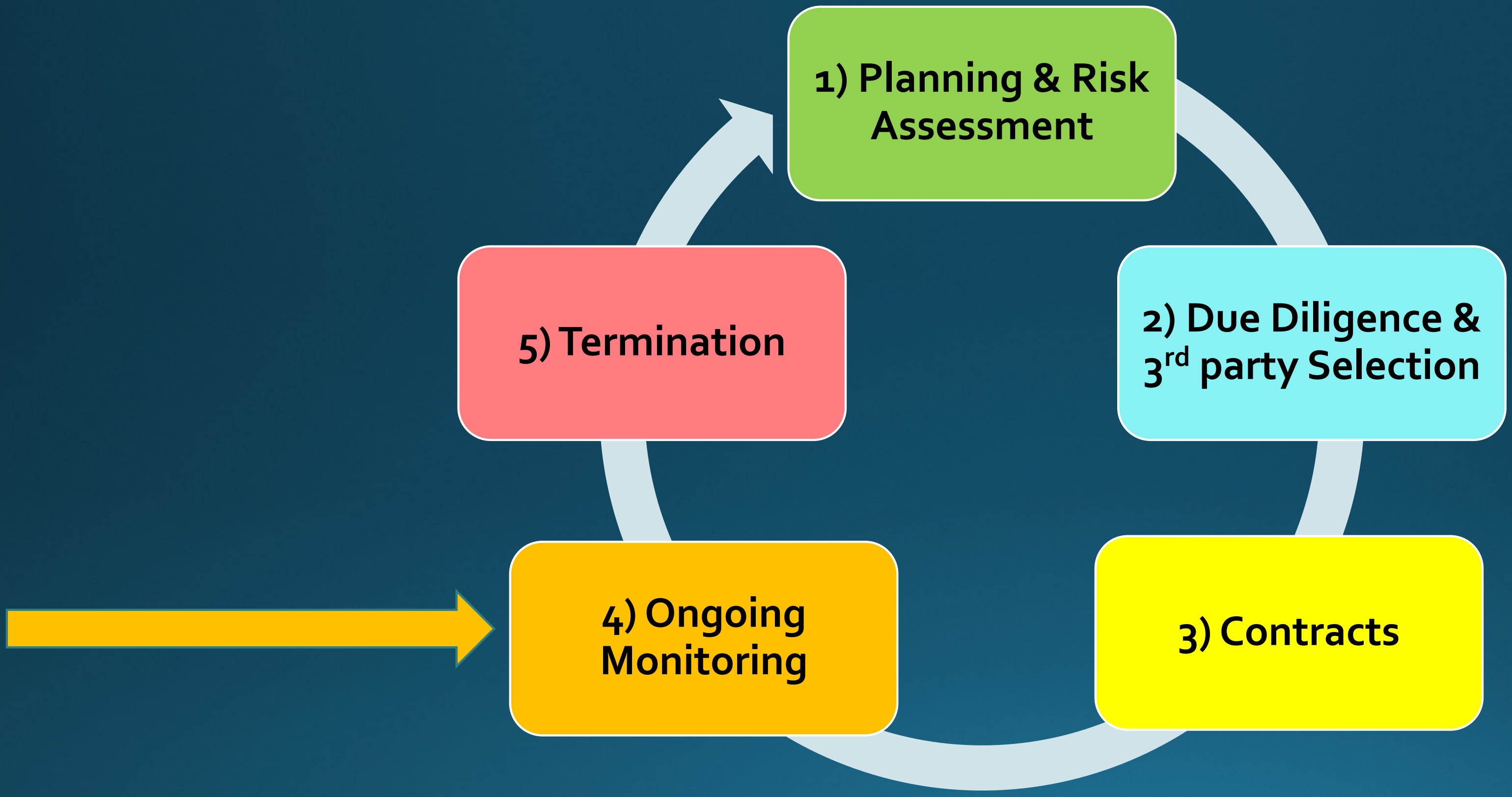
4) Ongoing Monitoring

5) Termination

3) Contracting

- Don’t willingly accept their standard contract
- Business Continuity and Disaster Recovery
- Data ownership and liability
- Information security and privacy requirements (including breach notification, accountability and responsibility for damages)
- Provisions for indemnification and their insurance
- Right to audit (questionnaires, interviews, audits)
- Ensure clarity on scope of services and measurable outcomes
- Ensure detailed service level agreements
- Subcontractor relationships (their third parties, our fourth-parties)
- Termination events

5 Phases of Third-Party Monitoring



1) Planning & Risk Assessment
2) Due Diligence & 3rd party Selection
3) Contracts
4) Ongoing Monitoring
5) Termination

Robert Clark, Jr., CCEP, CIA, CBM, Chief Audit & Compliance Officer, Howard University © 2023

4) Ongoing Monitoring

- For critical third-parties, regulators (e.g., Dept. of Education) expect:
  - Protection of data
  - Due diligence specific and commensurate to each vendor
  - Robust monitoring (especially over cybersecurity)
  - Holding vendor accountable to adhere to terms and conditions
  - Escalating issues on non-conformance
  - Documentation and reports of activities

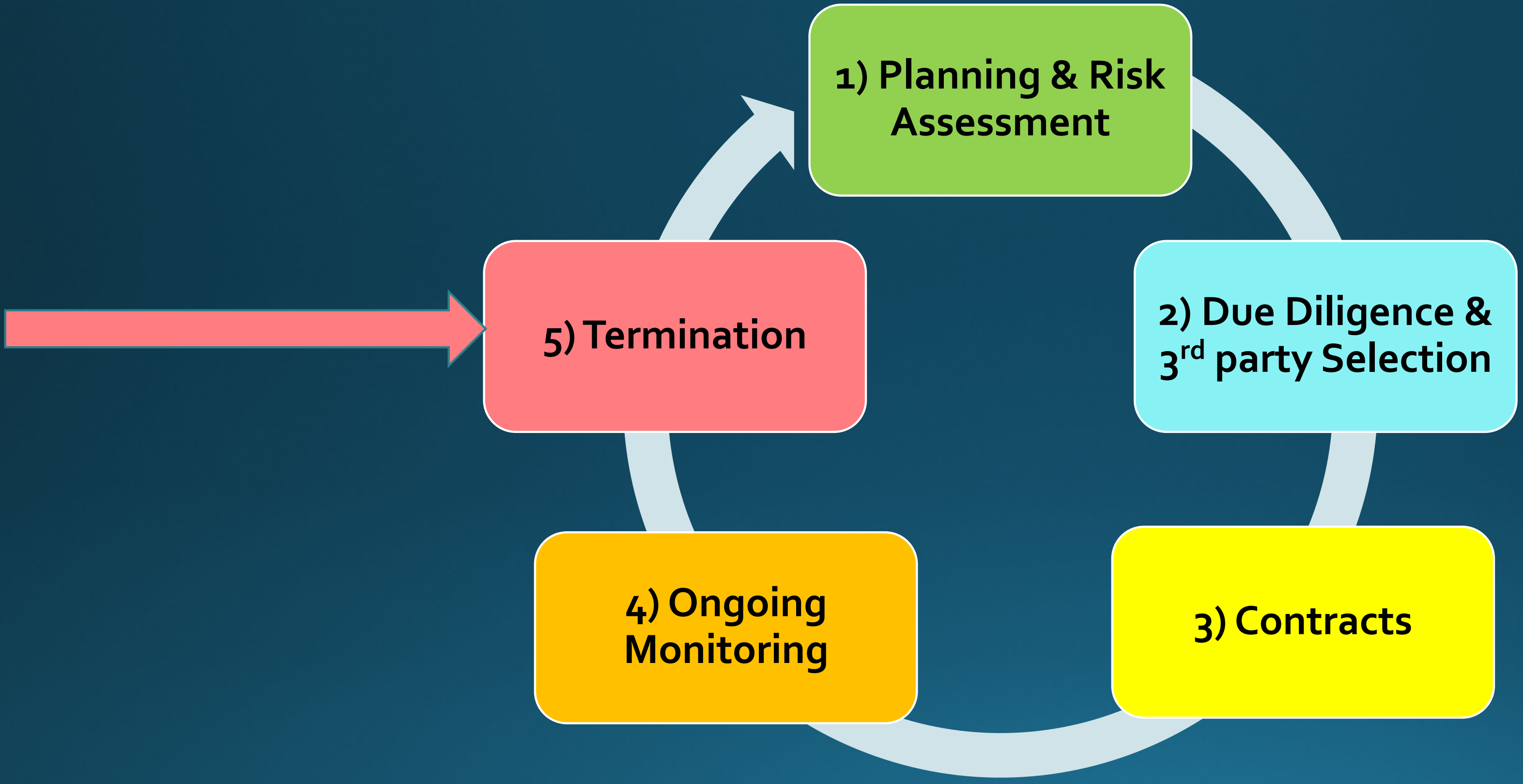
4) Ongoing Monitoring

- Continuous monitoring
- Point-in-time monitoring
- Over period-of-time monitoring
- Risk **re-**assessments
- Structured third-party offboarding

4) Ongoing Monitoring – What to Monitor

- Business strategy and reputation
- Compliance with legal and regulatory requirements
- Information security posture
- Controls over our data (confidentiality and integrity)
- Responsiveness to new threats
- Financial health
- Their management and mitigation of risk
- Retaining of key personnel
- Change in their reliance on their third-parties (our fourth-parties)

5 Phases of Third-Party Monitoring



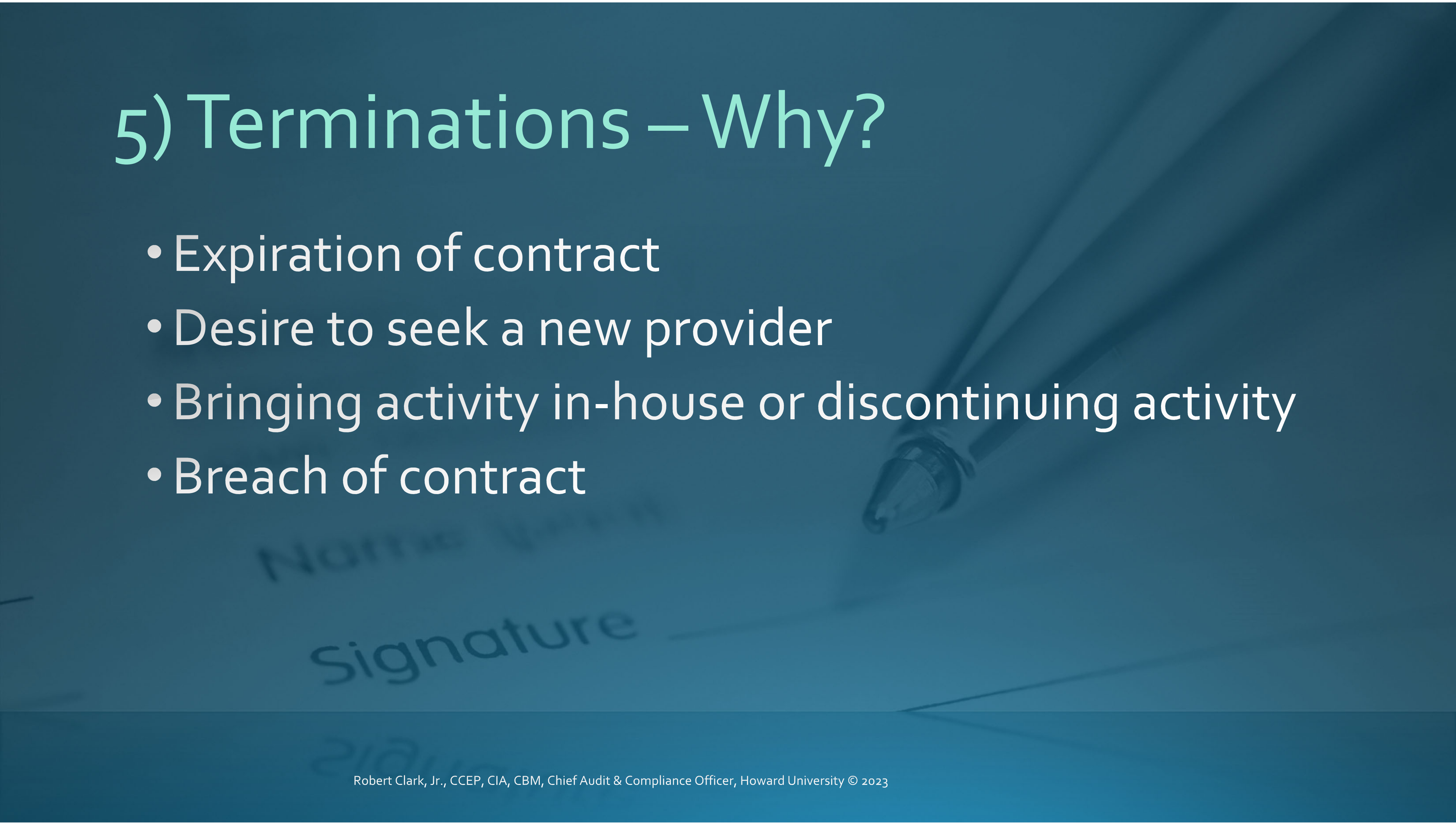
1) Planning & Risk Assessment

2) Due Diligence & 3rd party Selection

3) Contracts

4) Ongoing Monitoring

5) Termination



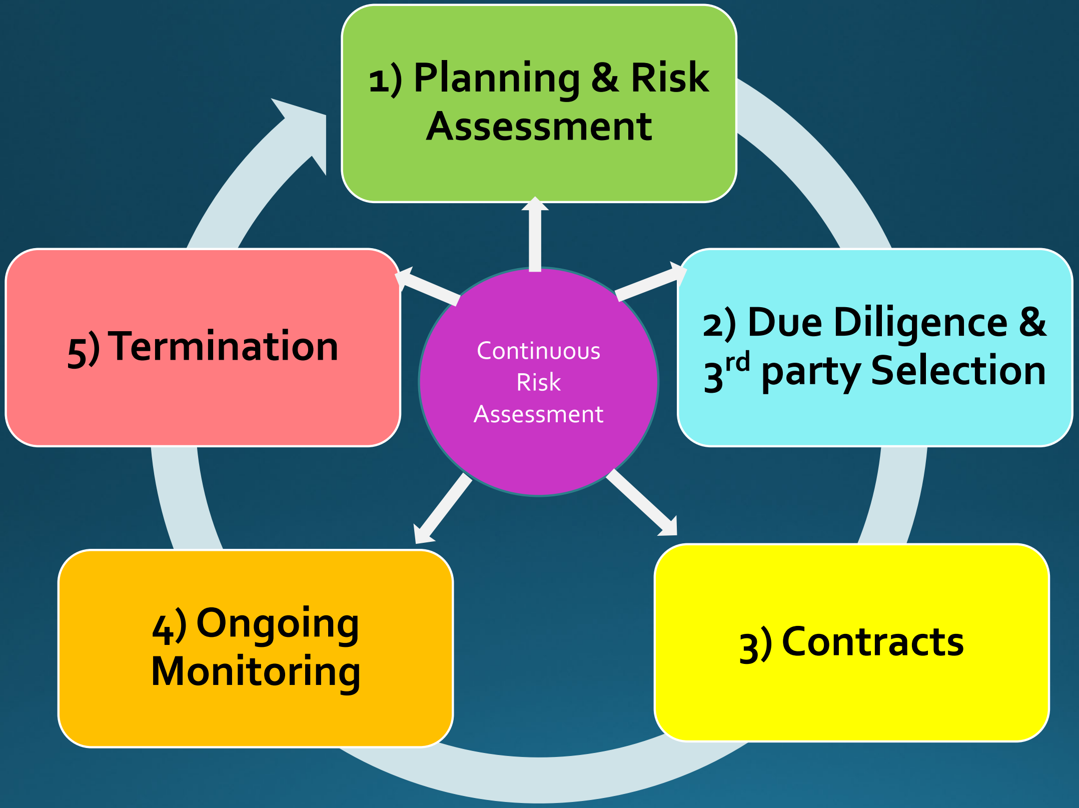
5) Terminations – Why?

- Expiration of contract
- Desire to seek a new provider
- Bringing activity in-house or discontinuing activity
- Breach of contract

5) Termination – Have a Plan, Build Into Contract

- What timeline and resources will be required to transition activity?
- Risks with data retention and destruction
- Info Systems access control issues
- Handling of intellectual property developed
- Reputation risks

5 Phases of Third-Party Monitoring



1) Planning & Risk Assessment

2) Due Diligence & 3rd party Selection

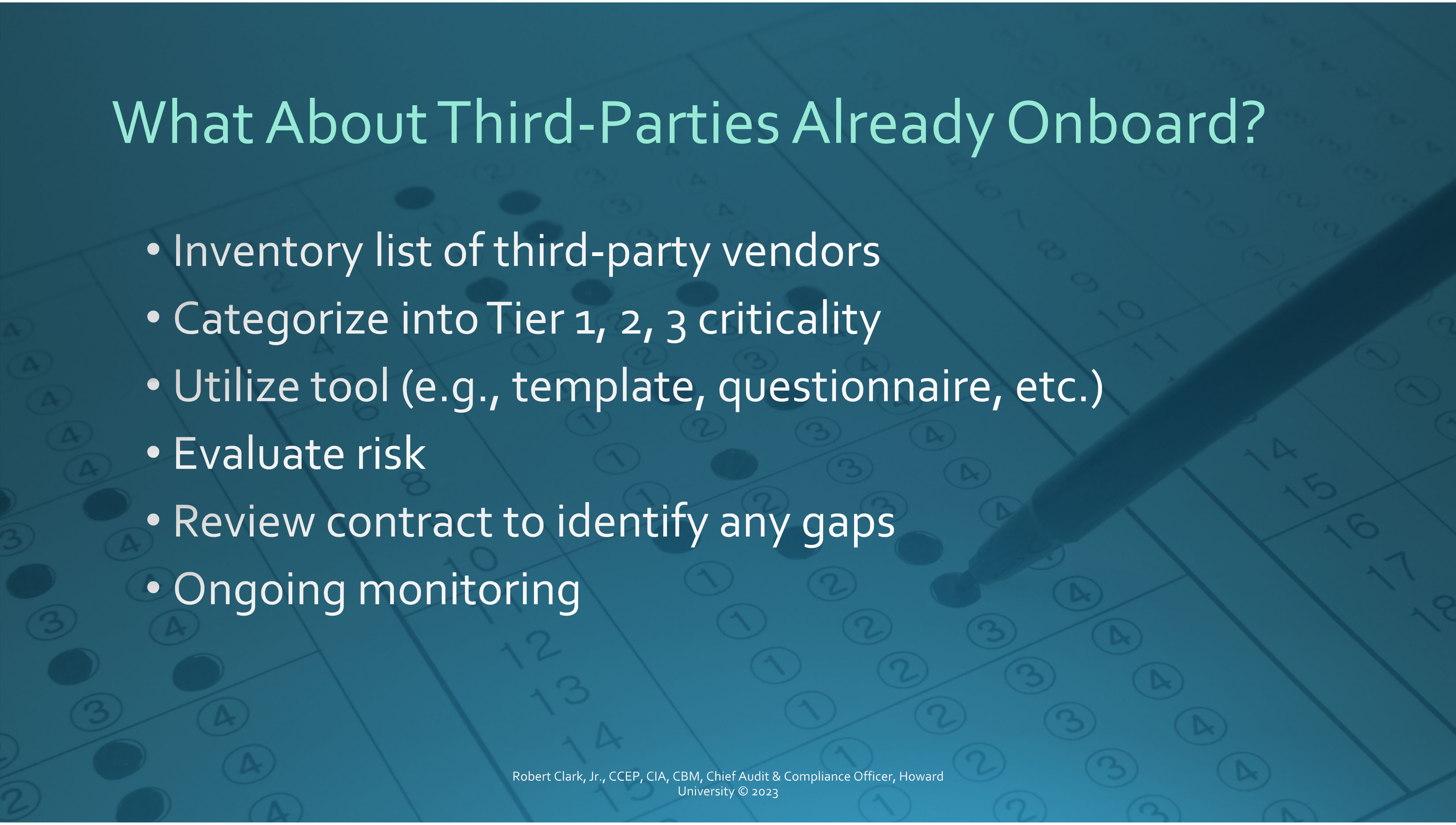
3) Contracts

4) Ongoing Monitoring

5) Termination

Continuous Risk Assessment

Robert Clark, Jr., CCEP, CIA, CBM, Chief Audit & Compliance Officer, Howard University © 2023



What About Third-Parties Already Onboard?

- Inventory list of third-party vendors
- Categorize into Tier 1, 2, 3 criticality
- Utilize tool (e.g., template, questionnaire, etc.)
- Evaluate risk
- Review contract to identify any gaps
- Ongoing monitoring

Polling Question 4:
What are the next steps for YOU?

A. Evaluate the processes to manage third-parties to identify risks

B. Reach out to Purchasing and Legal to find out how many third-parties you have

C. Talk with IT about implementing an IT Governance policy and council

D. Jump in with both feet and initiate a Third-Party Risk Management internal audit

What do I do with this info?

- Honest evaluation of your institution’s TPRM posture
- Engage internal stakeholders to identify gaps
- Facilitate discussions to determine actionable steps to enhance the TPRM posture
- Identify opportunities to establish/enhance policies and procedures
- Incorporate education and awareness
- Collaborate with Internal Audit, Compliance (those with responsibilities to report to executive leadership and the Board
- Get Board and executive leadership buy-in and support of resources needed to address gaps in TPRM

Discussion & Take-Aways

Rob Clark, Jr., CIA, CCEP, CBM
Chief Audit & Compliance Officer
Howard University
Robert.Clark@howard.edu
https://www.linkedin.com/in/robclarkjr/
www.RobClarkJr.com
770.815.7922

Announcements

Upcoming ACUA Webinars

Month	Date	Topic
July	7/27/23	Athletics
August	8/17/23	Lab Safety

See the ACUA website for more details
www.ACUA.org

ACUA WEBINARS

New Kick Starter Available!

IT Disaster Recovery

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

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

ACUA WEBINARS

Next Kick Starter Release is July 15th!

Fraud Risk Assessments

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

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

ACUA WEBINARS

CONNECT WITH US

ACUA
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

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:

AuditCon
September 2023
Miami, FL

- 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 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.